SOPHOS

SafeGuard® Enterprise 5.50

Aide administrateur

Date du document : Novembre 2010

Table des matières

1 SafeGuard Enterprise Management Center 3

2 Étapes de travail dans Management Center 6

3 Création de la structure organisationnelle 9

4 Utilisation de plusieurs configurations de base de données 21

5 Exportation des certificats de l'entreprise et du responsable principal de la sécurité 26

6 Licences 30

7 Responsables de la sécurité de SafeGuard Enterprise 39

8 Chiffrement de données 59

9 Gestion des clés de SafeGuard Enterprise 63

10 Utilisation de stratégies 74

11 Utilisation de packages de configuration 90

12 Options d'accès administratif sur les ordinateurs finaux 91

13 Listes de comptes de service pour la connexion Windows 92

14 Comptes d'accès POA pour la connexion POA sur des ordinateurs finaux non gérés 98

15 Stratégies de sécurité 104

16 SafeGuard Configuration Protection 150

17 Attribution utilisateur/ordinateur 184

18 Clés cryptographiques et cartes à puce 189

19 SafeGuard Data Exchange 209

20 Authentification au démarrage (POA) 218

21 Options de récupération 231

22 Récupération via Local Self Help 232

23 Récupération via Challenge/Réponse 238

24 Récupération du système 263

25 Données d'inventaire et d'état 269

26 Rapports 276

27 SafeGuard Enterprise et BitLocker Drive Encryption 291

28 SafeGuard Enterprise et BitLocker To Go 296

29 Événements disponibles pour les rapports 298

30 Définition des codes SGMERR du journal des événements de Windows 309

31 Support technique 324

32 Copyright 325

1 SafeGuard Enterprise Management Center

SafeGuard Enterprise Management Center est l'instrument central qui permet d'effectuer toutes les activités d'administration.

SafeGuard Management Center permet de desservir plusieurs bases de données et domaines par le biais de configurations spécifiques du titulaire (Multi Tenancy). Vous pouvez gérer plusieurs bases de données SafeGuard Enterprise et différentes configurations. Ces configurations peuvent également être exportées et importées pour simplifier la configuration.

SafeGuard Enterprise Management Center ne doit pas être installé nécessairement sur un seul ordinateur uniquement. Il peut être installé sur n'importe quel ordinateur du réseau permettant d'accéder aux bases de données.

Seuls les utilisateurs disposant des privilèges (les responsables de la sécurité) peuvent accéder à SafeGuard Management Center. Plusieurs responsables de la sécurité peuvent travailler simultanément avec les données.

1.1 Connexion à SafeGuard Management Center

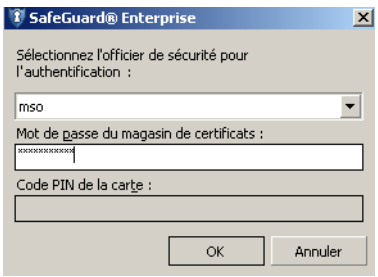
Lors de l'installation et de la configuration de SafeGuard Enterprise, tous les paramètres de configuration essentiels sont définis et un compte est créé pour un responsable principal de la sécurité. Ce compte est nécessaire la première fois que vous vous connectez à SafeGuard Management Center. Pour démarrer Management Center, l'utilisateur doit connaître le mot de passe du magasin des certificats et disposer de la clé privée du certificat.

Pour plus d'informations, consultez le manuel d'installation.

La connexion dépend de l'exécution de SafeGuard Management Center en mode Single Tenancy ou Multi Tenancy.

1.1.1 Connexion en mode Single Tenancy

1. Démarrez SafeGuard Management Center via le menu **Démarrer**. Une boîte de dialogue de connexion s'affiche.



2. Connectez-vous en tant que MSO et saisissez le mot de passe du magasin de certificats spécifié pendant la configuration initiale. Cliquez sur **OK**.

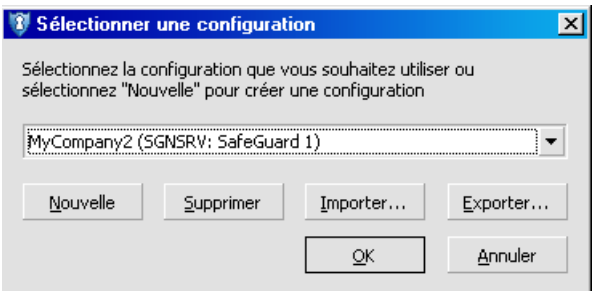
Remarque : si vous saisissez un mot de passe incorrect, un message d'erreur s'affiche et un délai est imposé avant la tentative de connexion suivante. Le délai est augmenté à chaque échec de tentative de connexion. Les échecs sont consignés.

SafeGuard Management Center est ouvert.

1.1.2 Connexion en mode Multi Tenancy

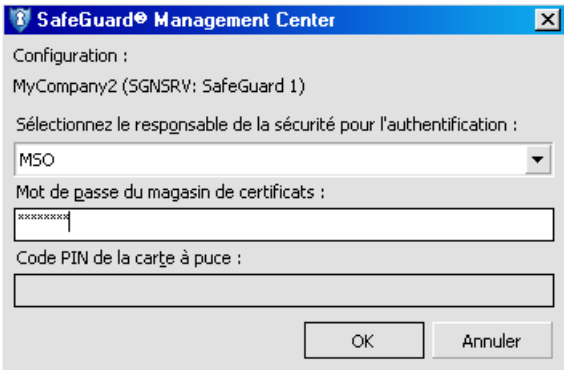
Le processus de connexion à Management Center est plus long lorsque plusieurs bases de données ont été configurées (Multi Tenancy), voir *Utilisation de plusieurs configurations de base de données* en page 21.

1. Démarrez SafeGuard Management Center via le dossier du produit dans le menu **Démarrer**. La boîte de dialogue **Sélectionner une configuration** s'affiche.



2. Sélectionnez la configuration de base de données que vous souhaitez utiliser dans la liste déroulante et cliquez sur **OK**. La configuration de base de données sélectionnée est reliée à Management Center et activée.

3. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Confirmez en cliquant sur **OK**.


SafeGuard® Management Center
Configuration :
MyCompany2 (SGNSRV: SafeGuard 1)
Sélectionnez le responsable de la sécurité pour l'authentification :
MSO
Mot de passe du magasin de certificats :
Code PIN de la carte à puce :
OK
Annuler

SafeGuard Management Center est ouvert et relié à la configuration de base de données sélectionnée.

Remarque : si vous saisissez un mot de passe incorrect, un message d'erreur s'affiche et un délai est imposé avant la tentative de connexion suivante. Le délai est augmenté à chaque échec de tentative de connexion. Les échecs sont consignés.

2 Étapes de travail dans Management Center

Les étapes suivantes sont essentielles pour utiliser SafeGuard Enterprise afin de garantir que les stratégies de sécurité à l'échelle de l'entreprise peuvent être appliquées aux ordinateurs finaux :

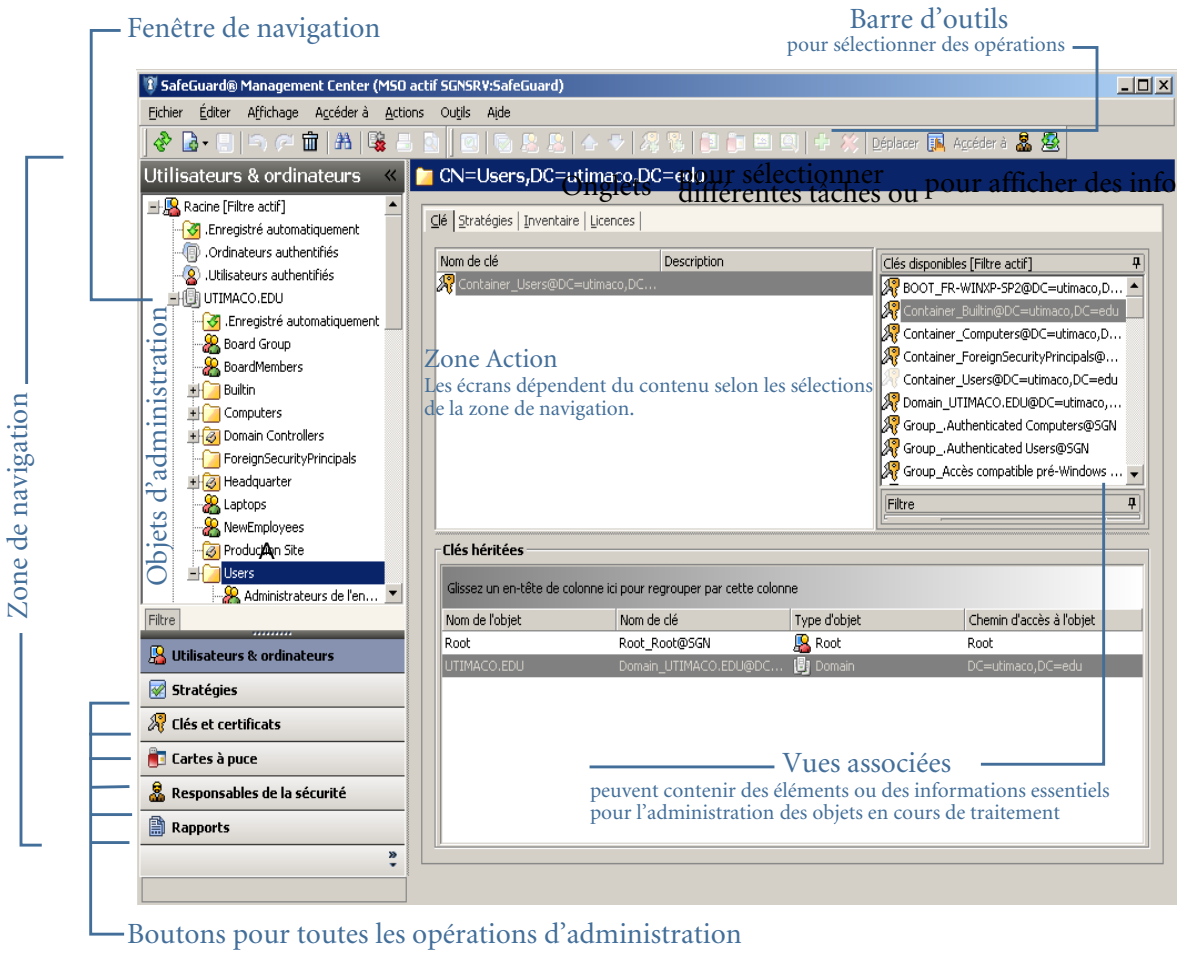
- création ou importation de la structure organisationnelle ;
- création des responsables de la sécurité supplémentaires ;
- définition des éléments de stratégies initiales (de base) ;
- enregistrement dans la base de données ;
- exportation et importation de configurations.

Utilisation quotidienne

Après la première connexion, des paramètres peuvent être ajoutés en fonction des besoins. Les différents responsables de la sécurité peuvent effectuer leurs opérations conformément aux rôles qui leur ont été attribués.

Si de nouveaux paramètres sont enregistrés dans la base de données, ils peuvent être transférés aux ordinateurs finaux, où ils deviennent actifs.

2.1 Zone de travail de Management Center


Fenêtre de navigation
Barre d'outils
pour sélectionner des opérations
Onglets pour sélectionner différentes tâches ou pour afficher des info
Zone de navigation
Objets d'administration
Zone Action
Les écrans dépendent du contenu selon les sélections de la zone de navigation.
Vues associées
peuvent contenir des éléments ou des informations essentiels pour l'administration des objets en cours de traitement
Boutons pour toutes les opérations d'administration

Zone de navigation

La zone de navigation contient des boutons pour toutes les opérations d'administration :

- Utilisateurs & ordinateurs

  Pour importer des groupes et des utilisateurs à partir d'un annuaire actif, à partir du domaine ou d'un ordinateur individuel.

- Stratégies

  Pour créer des éléments de stratégies.

- Clés et certificats

  Pour gérer les clés et les certificats.

- Cartes à puce

  Pour gérer les clés cryptographiques et les cartes à puce.

- Responsables de la sécurité

  Pour créer des responsables de la sécurité ou des rôles et définir les opérations qui nécessitent une autorisation supplémentaire.

- Rapports

  Permet la création d'enregistrements de tous les événements liés à la sécurité ainsi que leur gestion.

Fenêtre de navigation

Les objets devant être traités ou pouvant être créés sont affichés dans la fenêtre de navigation (objets Active Directory tels que les OU, utilisateurs et ordinateurs, éléments de stratégies, ...) selon la sélection des tâches d'administration.

Zone Action

Pour définir les paramètres des objets sélectionnés dans la fenêtre de navigation. La zone Action contient différents onglets permettant de traiter les objets et de définir les paramètres.

La zone Action comporte également des informations concernant les objets sélectionnés.

Vues associées

Dans ces vues, des objets et des informations supplémentaires sont affichés le cas échéant. Elles fournissent des informations utiles concernant l'administration du système et en simplifient l'utilisation. Par exemple, vous pouvez attribuer des clés en faisant glisser et en déposant des objets.

Barre d'outils

Contient des symboles relatifs aux différentes opérations de Management Center. Les symboles sont affichés tels qu'ils sont disponibles et quand ils sont disponibles pour l'objet sélectionné.

Après la connexion, Management Center s'ouvre toujours avec la vue qui était utilisée lors de sa fermeture.

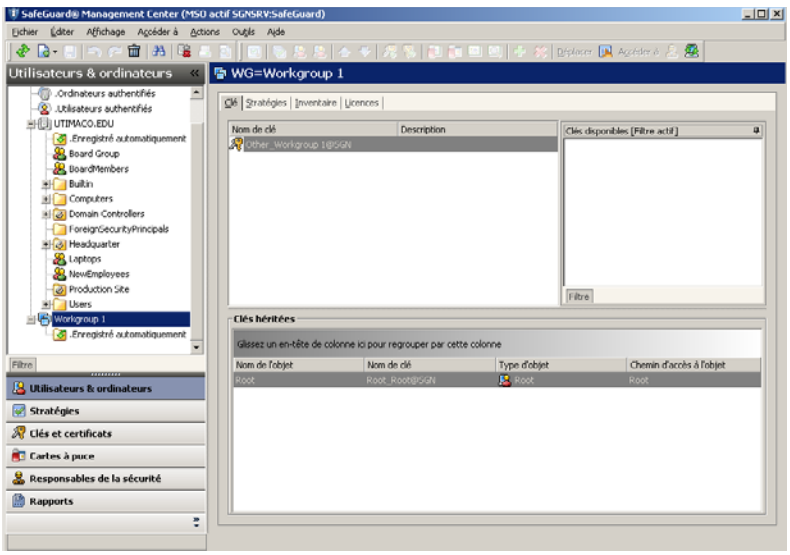
3 Création de la structure organisationnelle

Les utilisateurs et les ordinateurs peuvent également être définis dans SafeGuard Enterprise et ne doivent pas nécessairement être importés à partir d'Active Directory. En l'absence d'une structure organisationnelle existante, il est possible de la créer rapidement dans SafeGuard Enterprise avec une structure permettant de gérer des éléments de stratégies. Il est également possible d'attribuer des stratégies et/ou des règles de chiffrement aux utilisateurs locaux.

Un responsable de la sécurité doté des droits correspondants peut définir des groupes de travail ou des domaines qui n'ont pas encore été importés pour gérer les utilisateurs et les ordinateurs enregistrés automatiquement.

Les nouveaux utilisateurs et ordinateurs qui se connectent à SafeGuard Enterprise sont affichés sous leurs conteneurs correspondants après la synchronisation initiale avec la base de données dans SafeGuard Management Center. Les responsables de la sécurité peuvent ensuite les gérer exactement comme des objets importés.

Le répertoire de ces utilisateurs/ordinateurs, .Auto registered, est créé automatiquement dans le répertoire racine et sous chaque domaine/groupe de travail. Il ne peut être ni renommé ni déplacé. Les objets attribués à ce répertoire ne peuvent pas non plus être déplacés manuellement.



3.1 Enregistrement d'un nouvel utilisateur

Lorsqu'un nouvel utilisateur se connecte pour la première fois à SafeGuard Enterprise, l'état de sa base de données est vérifié au cours de la synchronisation initiale avec la base de données et le nouvel objet est affiché sous le conteneur correspondant, conformément aux informations de la base de données. Si aucun groupe de travail ou domaine nouveau n'a été créé, le nouvel utilisateur est ajouté à Auto.registered sous le répertoire racine. Si un domaine a déjà été créé sans que l'utilisateur/l'ordinateur n'aient encore été importés, ils sont ajoutés à Auto.registered sous le domaine.

Remarque : les utilisateurs locaux ne peuvent pas se connecter à SafeGuard Enterprise avec un mot de passe vide. Les utilisateurs locaux qui se connectent à SafeGuard Enterprise avec un mot de passe vide restent des invités et ne sont pas enregistrés dans la base de données. De plus, si la connexion automatique Windows est activée pour ces utilisateurs, la connexion leur est refusée. Pour se connecter à SafeGuard Enterprise, un nouveau mot de passe doit être créé et la connexion automatique Windows doit être désactivée dans le registre de l'ordinateur final.

Informations de connexion concernant l'objet local	État de la base de données :	Affiché dans SafeGuard Management Center
Utilisateurs locaux	Utilisateurs locaux inconnus	Sous le répertoire principal, .Auto registered nouvellement ajouté sous son ordinateur
Utilisateurs locaux, ordinateurs + domaines	Nœuds du domaine connus Utilisateurs/ordinateurs présents	Déjà présents sous les nœuds du domaine
	Nœuds du domaine connus Utilisateurs/ordinateurs non présents	.Auto registered nouvellement ajouté sous les nœuds du domaine

Informations de connexion concernant l'objet local	État de la base de données :	Affiché dans SafeGuard Management Center
Groupe de travail d'ordinateur + groupe de travail	Groupe de travail connu Utilisateurs/ordinateurs non présents physiquement	Déjà présent sous le groupe de travail
	Groupe de travail connu Nom des groupes de travail d'ordinateur présents sous .Auto registered	Nouvellement ajouté sous le groupe de travail .Auto registered **Avertissement :** Dans ce cas, vous devez vérifier si les groupes de travail d'ordinateur sont présents deux fois dans le groupe de travail. Pour différencier des ordinateurs identiques, accédez à **Propriétés** et saisissez la **Description**. Toutefois, nous vous recommandons de supprimer manuellement l'ordinateur du répertoire du groupe de travail .Auto registered.
	Groupe de travail connu Utilisateurs/ordinateurs non présents	Nouvellement ajouté sous le groupe de travail .Auto registered
	Groupe de travail inconnu Groupes de travail d'ordinateur connus sous le répertoire racine .Auto registered	Déjà présents sous le répertoire racine, .Auto registered
	Groupe de travail inconnu Groupes de travail d'ordinateur inconnus sous le répertoire racine .Auto registered	Nouvellement ajouté sous le répertoire racine .Auto registered
Domaines d'ordinateur + domaines	Domaine connu Domaines d'ordinateur présents	Déjà présent sous le domaine
	Domaine inconnu	Nouvellement ajouté sous le répertoire racine .Auto registered
	Domaine pas encore synchronisé	Nouvellement ajouté sous le domaine .Auto registered

3.2 Études de cas de l'enregistrement automatique

Vous trouverez ci-après deux études de cas du comportement d'objets enregistrés automatiquement.

Étude de cas 1 : Gestion d'utilisateurs/ordinateurs ne faisant pas partie d'un Active Directory

Dans une entreprise, tous les objets utilisateur ou ordinateur ne font pas nécessairement partie d'un Active Directory (AD), les utilisateurs locaux par exemple. Une entreprise peut disposer d'un ou de quelques groupes de travail, un AD n'est donc pas nécessaire.

Cette entreprise souhaite déployer SafeGuard Enterprise, puis ajouter des stratégies à ses objets utilisateur/ordinateur. La structure organisationnelle de l'entreprise doit donc être créée manuellement dans SafeGuard Management Center comme suit :

Arborescence **Utilisateurs & ordinateurs** :

Racine

|_.Authenticated Computers

|_.Authenticated Users

|_.Auto registered

|_**SampleWorkgroup** (entrée ajoutée manuellement)

|_.Auto registered

|_**SampleComputer001**
(entrée créée à la connexion)

|_**SampleComputer002**
(entrée créée à la connexion)

|_...

Les objets utilisateur et ordinateur restent dans le dossier .Auto registered. Ils peuvent cependant être gérés via SafeGuard Management Center (ajout ou suppression de stratégies, etc.).

Étude de cas 2 : Base de données de SafeGuard Enterprise et Active Directory non synchronisés

Un utilisateur et un ordinateur (client SafeGuard Enterprise) font déjà partie de l'AD (Active Directory) de l'entreprise. La base de données de SafeGuard Enterprise et l'AD ne sont cependant pas synchronisés : l'utilisateur et l'ordinateur ne sont pas répertoriés dans SafeGuard Management Center.

L'utilisateur se connecte à l'ordinateur (client SafeGuard Enterprise) avec les informations d'identification suivantes :

SampleUser

SamplePassword

Sample Domain

Ces informations sont transmises au serveur SafeGuard Enterprise. Dans SafeGuard Management Center, les entrées suivantes sont créées :

Arborescence **Utilisateurs & ordinateurs** :

Racine

|_.Authenticated Computers

|_.Authenticated Users

|_.Auto registered

|_**SampleDomain** (entrée créée en synchronisation avec l'AD)

|_.Auto registered

|_**SampleComputer**
(entrée créée à la connexion)

|_**SampleUser**
(entrée créée à la connexion)

Lors de la synchronisation suivante entre l'AD et la base de données de SafeGuard Enterprise, **SampleComputer** et **SampleUser** sont déplacés automatiquement dans les unités organisationnelles (OU) appropriées.

Le responsable principal de la sécurité (MSO) peut ajouter des stratégies au dossier .Auto registered s'il le souhaite mais ces stratégies ne s'appliqueront à **SampleComputer** et à **SampleUser** que si ces objets font partie du dossier .Auto registered.

Une fois déplacés dans leurs unités organisationnelles (OU) via une synchronisation entre l'AD et la base de données de SafeGuard Enterprise, les stratégies définies pour ces OU s'appliqueront à **SampleComputer** et à **SampleUser**.

3.3 Clés et certificats pour les objets enregistrés automatiquement

Un certificat est produit selon les besoins par le serveur pour chaque objet enregistré automatiquement.

Un utilisateur local obtient deux clés :

- la clé du conteneur .Auto registered
- la clé privée générée en fonction des besoins par le serveur

Les utilisateurs locaux n'obtiennent aucune autre clé pour leur conteneur attribué ni une clé racine.

Les groupes de travail n'obtiennent pas de clé.

3.4 Stratégies pour les objets enregistrés automatiquement

Des stratégies illimitées peuvent être créées pour les objets enregistrés automatiquement.

Les utilisateurs locaux sont ajoutés au groupe « Utilisateurs authentifiés ». Les ordinateurs sont ajoutés au groupe « Ordinateurs authentifiés ». Les stratégies activées pour ces groupes s'appliquent en conséquence.

3.5 Création d'un groupe de travail

Les responsables de la sécurité dotés des droits correspondants peuvent créer un conteneur sous le répertoire racine qui représente un groupe de travail Windows. Les groupes de travail n'ont pas de clé. Ils ne peuvent pas être renommés.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs**.
2. Cliquez avec le bouton droit sur **Racine** [**Filtre actif**] dans la fenêtre de navigation de gauche et sélectionnez **Nouveau** > **Créer un groupe de travail** (**enregistrement auto**).
3. Dans **Informations communes** spécifiez les éléments suivants :
   a) Entrez un **nom complet** pour le groupe de travail.
   b) Vous pouvez éventuellement ajouter une **description** du groupe de travail.
   c) Le type d'objet est affiché sous **État de connexion**, dans ce cas `Groupe de travail`.
   d) Pour empêcher l'héritage de stratégie, vous pouvez activer **Bloquer l'héritage de stratégie**.
   e) Confirmez les détails en cliquant sur **OK**.

À présent, le groupe de travail est créé. Le répertoire .Auto registered par défaut est créé automatiquement sous le conteneur du groupe de travail. Il ne peut être ni renommé ni supprimé.

3.6 Suppression de groupes de travail

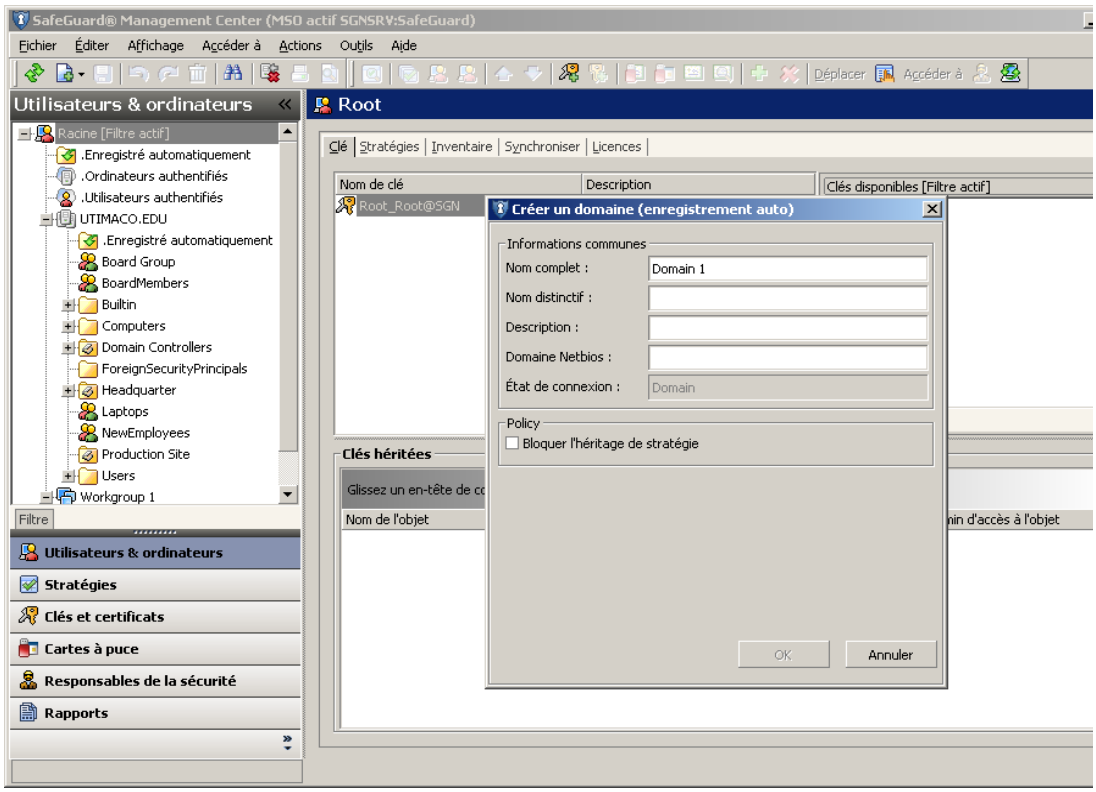
Les responsables de la sécurité peuvent supprimer des groupes de travail. Les membres appartenant au groupe de travail sont également supprimés. Ils sont réenregistrés automatiquement lors de la prochaine connexion.

1. Dans SafeGuard Management Center cliquez sur **Utilisateurs & ordinateurs**.
2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit sur le groupe de travail à supprimer puis sélectionnez **Supprimer. Confirmez** en cliquant sur **Oui**.

À présent, le groupe de travail est supprimé. Ses membres éventuels sont également supprimés.

3.7 Création d'un domaine

Les responsables de la sécurité dotés des droits correspondants peuvent créer un domaine sous le répertoire racine. Vous ne devez créer un nouveau domaine que si vous ne voulez pas ou ne pouvez pas importer un domaine à partir d'Active Directory (AD), par exemple du fait qu'aucun AD n'est disponible.



1. Dans SafeGuard Management Center cliquez sur **Utilisateurs & ordinateurs**.
2. Cliquez avec le bouton droit sur **Racine** [**Filtre actif**] dans la fenêtre de navigation de gauche et sélectionnez **Nouveau** > **Créer un domaine** (**enregistrement auto**).
3. Dans **Informations communes**, saisissez les informations suivantes concernant le contrôleur de domaine. La saisie des trois noms doit être correcte sinon le domaine ne sera pas synchronisé :
   a) **Nom complet** : par exemple *nom ordinateur.domaine.com* ou l'adresse IP du contrôleur de domaine.
   b) **Nom distinctif** : nom DNS, par exemple `DC=nomordinateur3,DC=domaine,DC=pays`
   c) Description du domaine (facultatif)
   d) **Netbios du domaine :** nom du contrôleur de domaine

e) Le type d'objet est affiché sous **État de la connexion**, dans ce cas `Domaine`.

f) Pour empêcher l'héritage de stratégie, vous pouvez activer **Bloquer l'héritage de stratégie**.

g) Confirmez les détails en cliquant sur **OK**.

Le domaine est à présent créé. Les utilisateurs et/ou ordinateurs sont automatiquement attribués à ce domaine au cours de l'enregistrement automatique. Le répertoire par défaut .Auto registered est créé automatiquement sous le conteneur du domaine. Il ne peut être ni renommé ni supprimé.

3.8 Changement de nom d'un domaine

Un responsable de la sécurité doté des droits correspondants peut renommer un domaine et définir des propriétés supplémentaires.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs.**
2. Cliquez avec le bouton droit sur le domaine que vous voulez renommer dans la fenêtre de navigation de gauche et sélectionnez **Propriétés**.
3. Dans **Informations communes**, sous **Nom complet**, changez le nom du domaine et éventuellement sa description.
4. Vous pouvez renommer le contrôleur de domaine dans **NetBios du domaine**.
5. Vous pouvez également définir le mode Éveil par appel réseau pour la réinitialisation automatique dans l'onglet **Paramètres de conteneur**.
6. Confirmez en cliquant sur **OK**.

À présent, les modifications sont enregistrées.

3.9 Suppression d'un domaine

Les responsables de la sécurité dotés des droits correspondants peuvent supprimer des domaines. Les membres appartenant au domaine sont également supprimés.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs.**
2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit sur le domaine à supprimer puis sélectionnez **Supprimer.** Confirmez en cliquant sur **Oui**.

À présent, le domaine est supprimé. Ses membres éventuels sont également supprimés.

3.10 Suppression des ordinateurs enregistrés automatiquement

Lorsqu'un ordinateur enregistré automatiquement est supprimé, tous les utilisateurs locaux de cet ordinateur le sont également. Ils sont réenregistrés automatiquement lors de leur prochaine connexion à cet ordinateur.

3.11 Filtre pour les objets locaux

Utilisateurs & ordinateurs

Dans **Utilisateurs & ordinateurs**, vous pouvez filtrer la vue de la fenêtre de navigation de gauche selon les utilisateurs locaux ou rechercher certains utilisateurs locaux.

1. Dans SafeGuard Management Center cliquez sur **Utilisateurs & ordinateurs**.
2. Dans la partie inférieure gauche de la fenêtre de navigation, cliquez sur **Filtrer**.
3. Activez **Utilisateur local** en tant que **Type**. Si vous recherchez un utilisateur particulier, saisissez son nom.
4. Cliquez sur l'icône de la loupe.

La vue **Utilisateurs & ordinateurs** est filtrée en fonction des critères.

Consignation

Réussite/échec de l'enregistrement de l'utilisateur, l'ordinateur ou le groupe de travail est connecté. Vous pouvez consulter la liste de ces informations dans SafeGuard Management Center sous **Rapports** dans la visionneuse des événements.

3.12 Importation de la structure organisationnelle à partir d'Active Directory

Vous avez la possibilité d'importer une structure organisationnelle existante dans la base de données SafeGuard Enterprise, par exemple via Active Directory.

1. Dans SafeGuard Management Center, sélectionnez **Outils** > **Options.**
2. Sélectionnez l'onglet **Répertoire** et cliquez sur **Ajouter**.

3. Dans **Authentification LDAP**, procédez comme suit :

   a) Pour **Nom ou adresse IP du serveur**, entrez le nom NETBIOS du contrôleur de domaine ou son adresse IP.

   b) Pour **Autorisations utilisateur**, entrez votre nom et votre mot de passe Windows pour vous connecter à l'environnement (test).

   c) Confirmez en cliquant sur **OK**.

Remarque : pour un ordinateur unique Windows, un répertoire doit être approuvé sur le PC pour activer une connexion via LDAP.

4. Cliquez sur **Utilisateurs & ordinateurs**.

5. Dans la fenêtre de navigation de gauche, cliquez sur le répertoire racine **Racine** [**Filtre actif**].

6. Sélectionnez l'onglet **Synchroniser** dans la zone d'action de droite.

7. Sélectionnez le répertoire requis dans la liste **DSN répertoire**. Cliquez sur l'icône de la loupe, en haut et à droite.
   Une représentation graphique de la structure Active Directory des unités organisationnelles (OU) de votre entreprise s'affiche.

8. Il n'est pas nécessaire d'importer l'ensemble du contenu d'Active Directory. Cochez les unités organisationnelles (OU) qui doivent être synchronisées.

9. Cliquez sur **Synchroniser** au bas de la zone d'action.

Remarque : lors de la synchronisation d'utilisateurs avec leur appartenance à un groupe, l'appartenance à un groupe « principal » n'est pas synchronisée car elle n'est pas visible pour le groupe.

Les domaines sont synchronisés. Des informations sur la synchronisation s'affichent. Vous pouvez afficher un protocole de synchronisation dans la barre d'état à gauche. En cliquant dessus, vous pouvez copier ce protocole dans le Presse-papiers et le coller dans un e-mail ou un fichier pour communiquer aux utilisateurs les résultats de la synchronisation.

3.13 Importation d'un nouveau domaine à partir d'Active Directory

Pour n'importer qu'un nouveau domaine à partir d'Active Directory, procédez de la façon suivante :

1. Dans la fenêtre de navigation de gauche, cliquez sur le répertoire racine **Racine** [**Filtre actif**].
2. Sélectionnez **Fichier** > **Nouveau** > **Importer nouveau domaine de AD**.
3. Sélectionnez l'onglet **Synchroniser** dans la zone d'action de droite.
4. Sélectionnez le répertoire requis dans la liste **DSN répertoire**. Cliquez sur l'icône de la loupe, en haut et à droite.
   Une représentation graphique de la structure Active Directory des unités organisationnelles (OU) de votre entreprise s'affiche.
5. Cochez le domaine à synchroniser et cliquez sur **Synchroniser** au bas de la zone de navigation.

4 Utilisation de plusieurs configurations de base de données

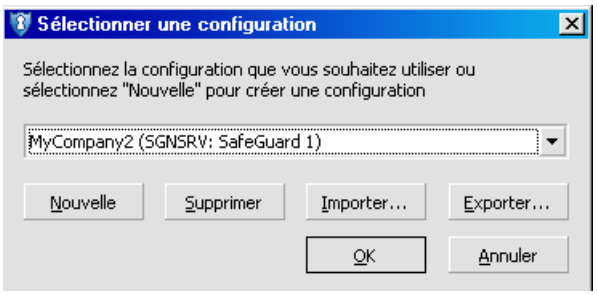
SafeGuard Management Center permet d'utiliser plusieurs configurations de base de données (plusieurs titulaires). Pour utiliser cette fonction, vous devez l'activer pendant l'installation. Pour plus d'informations, reportez-vous au manuel d'installation de SafeGuard Enterprise.

Le mode Multi Tenancy vous permet de configurer différentes configurations de base de données SafeGuard Enterprise et de les gérer pour une instance de SafeGuard Management Center. Ceci est tout particulièrement utile si vous souhaitez disposer de configurations différentes pour des domaines, des unités organisationnelles ou des lieux différents.

Condition préalable : La fonctionnalité Multi Tenancy doit avoir été installée via une installation de type Personnalisé. La configuration initiale doit être réalisée. Pour plus d'informations, reportez-vous au manuel d'installation de SafeGuard Enterprise.

Pour simplifier la configuration, les tâches suivantes sont possibles :

- créer plusieurs configurations de base de données ;
- sélectionner dans une liste de configurations de base de données créées précédemment ;
- importer une configuration de base de données créée précédemment à partir d'un fichier ;
- exporter une configuration de base de données à réutiliser ultérieurement.



4.1 Création de configurations de base de données supplémentaires

Pour créer d'autres configurations de base de données SafeGuard Enterprise à la suite de la configuration initiale, veuillez procéder comme suit :

1. Démarrez SafeGuard Management Center. La boîte de dialogue **Sélectionner une configuration** s'affiche.
2. Cliquez sur **Nouvelle**. L'assistant de configuration de SafeGuard Management Center se lance automatiquement.

3. L'assistant vous guide dans les étapes nécessaires de création d'une configuration de base de données. Définissez les paramètres tels que requis. La nouvelle configuration de base de données est générée.

4. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Confirmez en cliquant sur **OK**.

SafeGuard Management Center est ouvert et relié à la nouvelle configuration de base de données. Au prochain lancement de SafeGuard Management Center, la nouvelle configuration de base de données peut être sélectionnée dans la liste.

4.2 Association à une configuration de base de données existante

Pour travailler sur une configuration de base de données SafeGuard Enterprise, veuillez procéder comme suit :

1. Démarrez SafeGuard Management Center. La boîte de dialogue **Sélectionner une configuration** s'affiche.

2. Sélectionnez la configuration de base de données souhaitée dans la liste déroulante et cliquez sur **OK**. La configuration de base de données sélectionnée est reliée à Management Center et activée.

3. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Confirmez en cliquant sur **OK**.

SafeGuard Management Center est ouvert et relié à la configuration de base de données sélectionnée.

4.3 Exportation d'une configuration dans un fichier

Pour enregistrer ou réutiliser une configuration de base de données, vous pouvez l'exporter dans un fichier. Pour cela, veuillez procéder comme suit :

1. Démarrez SafeGuard Management Center. La boîte de dialogue **Sélectionner une configuration** s'affiche.

2. Cliquez sur **Exporter...**.

3. Pour protéger le fichier de configuration, vous êtes invité à saisir et confirmer un mot de passe qui chiffrera le fichier de configuration. Cliquez sur **OK**.

4. Spécifiez un nom de fichier et un emplacement de stockage pour le fichier de configuration exportée *.SGNConfig.
5. Si cette configuration existe déjà, vous êtes invité à confirmer le remplacement de la configuration existante.

La configuration de base de données est enregistrée à l'emplacement de stockage spécifié.

4.4 Importation d'une configuration à partir d'un fichier

Pour utiliser ou modifier une configuration de base de données, vous pouvez importer une configuration créée précédemment dans SafeGuard Management Center. Pour ce faire, vous pouvez procéder de deux façons :

- via SafeGuard Management Center (Multi Tenancy) ;
- en double-cliquant sur le fichier de configuration (Single et Multi Tenancy).

4.5 Importation d'une configuration via SafeGuard Management Center

1. Démarrez SafeGuard Management Center. La boîte de dialogue **Sélectionner une configuration** s'affiche.
2. Cliquez sur **Importer...**, recherchez le fichier de configuration souhaité, puis cliquez sur **Ouvrir**.
3. Entrez le mot de passe du fichier de configuration défini lors de l'exportation, puis cliquez sur **OK**.
4. La configuration sélectionnée s'affiche. Confirmez pour l'activer en cliquant sur **OK**.
5. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Confirmez en cliquant sur **OK**.

SafeGuard Management Center est ouvert et relié à la configuration de base de données importée.

4.6 Importation d'une configuration en double-cliquant sur le fichier de configuration (Single et Multi Tenancy)

Remarque : notez que cette tâche est disponible en mode Single Tenancy et Multi Tenancy.

Il est également possible d'exporter une configuration et de la distribuer vers plusieurs responsables de la sécurité. Les responsables de la sécurité double-cliquent alors simplement sur le fichier de configuration pour ouvrir une instance SafeGuard Management Center totalement configurée.

Ceci est avantageux lorsque vous utilisez l'authentification SQL pour la base de données et pour éviter que chaque administrateur connaisse le mot de passe SQL. Vous ne le saisissez ensuite qu'une seule fois, vous créez un fichier de configuration et vous le distribuez vers les ordinateurs des responsables de la sécurité concernés.

Condition préalable : La configuration initiale de SafeGuard Management Center doit avoir été effectuée. Pour plus d'informations, reportez-vous au manuel d'installation de SafeGuard Enterprise.

1. Démarrez SafeGuard Management Center par l'intermédiaire du dossier du produit dans le menu **Démarrer**.
2. Sélectionnez **Options** dans le menu **Outils**, puis cliquez sur l'onglet **Base de données**.
3. Saisissez et confirmez les informations d'identification de la connexion au serveur de base de données SQL.
4. Cliquez sur **Exporter la configuration** pour exporter cette configuration vers un fichier.
5. Entrez et confirmez le mot de passe du fichier de configuration.
6. Entrez un nom de fichier et spécifiez un emplacement de stockage.
7. Distribuez ce fichier de configuration vers les ordinateurs des responsables de la sécurité. Fournissez-leur le mot de passe de ce fichier et du magasin de certificats nécessaires pour s'authentifier dans SafeGuard Management Center.
8. Les responsables de la sécurité double-cliquent simplement sur le fichier de configuration.
9. Ils sont invités à saisir le mot de passe du fichier de configuration.
10. Pour s'authentifier à SafeGuard Management Center, ils sont invités à saisir leur mot de passe de magasin de certificats.

SafeGuard Management Center démarre avec la configuration importée et celle-ci devient la nouvelle configuration par défaut.

4.7 Basculement rapide entre les configurations de base de données

Pour simplifier la gestion de plusieurs titulaires, SafeGuard Management Center permet de basculer rapidement entre les configurations de base de données.

Pour passer à une autre configuration de base de données :

1. Dans Management Center, sélectionnez **Changer la configuration...** dans le menu **Fichier**.
2. Dans la liste déroulante, sélectionnez la base de données à laquelle vous souhaitez accéder et confirmez votre choix en cliquant sur **OK**.

SafeGuard Management Center redémarre automatiquement avec la configuration sélectionnée.

Avis : cette tâche est également disponible en mode Single Tenancy.

4.8 Vérification de l'intégrité de la base de données

Lorsque vous vous connectez à la base de données, l'intégrité de cette dernière est vérifiée automatiquement. La boîte de dialogue **Vérifier l'intégrité de la base de données** s'affiche si cette vérification renvoie des erreurs.

Vous pouvez également lancer la vérification de l'intégrité de la base de données et afficher la boîte de dialogue **Vérifier l'intégrité de la base de données** :

1. Sélectionnez **Outils** > **Intégrité base de données** dans la barre de menus de SafeGuard Management Center.
2. Vérifiez les tables en cliquant sur **Tout vérifier** ou **Vérifier sélection**. Les tables erronées sont indiquées dans la boîte de dialogue.

Pour les réparer, cliquez sur **Réparer**.

5 Exportation des certificats de l'entreprise et du responsable principal de la sécurité

Dans une installation SafeGuard Enterprise, les deux éléments suivants sont essentiels et nécessitent une sauvegarde approfondie sur un emplacement sûr :

- le certificat de la société enregistré dans la base de données SafeGuard ;
- le certificat du responsable principal de la sécurité (MSO) se trouvant dans le magasin de certificats de l'ordinateur sur lequel SafeGuard Management Center est installé.

Ces deux certificats peuvent être exportés sous la forme de fichiers .p12 à des fins de sauvegarde. Les installations peuvent ensuite être restaurées en important le certificat de la société et du responsable de la sécurité sous forme de fichiers .p12. Utilisez-les au moment de configurer une nouvelle base de données plutôt que de devoir sauvegarder et restaurer l'ensemble de celle-ci.

Remarque: Nous conseillons de réaliser cette tâche immédiatement après la configuration initiale de SafeGuard Management Center.

5.1 Exportation du certificat du responsable principal de la sécurité

Pour sauvegarder le certificat du responsable principal de la sécurité connecté à SafeGuard Management Center, procédez comme suit :

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Options**.
2. Cliquez sur l'onglet **Certificats**, puis sur **Exporter** dans la section **Certificat <Administrateur>**.
3. Vous êtes invité à saisir un mot de passe pour sécuriser le fichier exporté. Entrez un mot de passe, confirmez-le, puis cliquez sur **OK**.
4. Saisissez un nom et un emplacement de stockage pour le fichier à exporter, puis cliquez sur **OK** pour confirmer.

Le certificat du responsable principal de la sécurité actuellement connecté est exporté sous la forme d'un fichier .p12 à l'emplacement défini et peut être utilisé à des fins de récupération.

5.2 Exportation des certificats d'entreprise

Remarque: Seuls les responsables principaux de la sécurité sont autorisés à exporter les certificats de la société à des fins de sauvegarde.

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Options**.
2. Cliquez sur l'onglet **Certificats**, puis sur **Exporter** dans la section **Certificat d'entreprise**.
3. Vous êtes invité à saisir un mot de passe pour sécuriser le fichier exporté. Entrez un mot de passe, confirmez-le, puis cliquez sur **OK**.
4. Saisissez un nom et un emplacement de stockage pour le fichier, puis cliquez sur **OK**.

Le certificat de la société est exporté sous la forme d'un fichier .p12 à l'emplacement désigné et peut être utilisé à des fins de récupération.

5.3 Restauration d'une installation corrompue de SafeGuard Management Center

Si l'installation de SafeGuard Management Center est corrompue mais que la base de données est intacte, l'installation peut facilement être restaurée en réinstallant SafeGuard Management Center et en utilisant la base de données existante ainsi que le certificat du responsable de la sécurité sauvegardé.

Procédez comme suit :

1. Installez le package d'installation de SafeGuard Management Center. Ouvrez SafeGuard Management Center. L'assistant de configuration démarre automatiquement.
2. Dans **Connexion à la base de données**, sélectionnez le serveur de base de données correspondant et configurez la connexion à la base de données, le cas échéant. Cliquez sur **Suivant**.
3. Dans **Paramètres de base de données**, activez **Sélectionner une base de données disponible** et sélectionnez dans la liste la base de données correspondante.

4. Dans **Responsable de la sécurité**, exécutez l'une des actions suivantes :
   - Si le fichier de certificat sauvegardé se trouve sur l'ordinateur, il s'affiche. Entrez le mot de passe utilisé pour vous authentifier pour SafeGuard Management Center.
   - Si le fichier de certificat sauvegardé est introuvable sur l'ordinateur, cliquez sur **Importer**. Recherchez le fichier de certificat sauvegardé et cliquez sur **Ouvrir** pour confirmer. Saisissez le mot de passe du fichier de certificat sélectionné. Cliquez sur **Oui** pour confirmer. Entrez et confirmez un mot de passe pour vous authentifier pour SafeGuard Management Center.
5. Cliquez sur **Suivant**, puis sur **Terminer** pour terminer la configuration de SafeGuard Management Center.

L'installation corrompue de SafeGuard Management Center est restaurée.

5.4 Restauration d'une configuration corrompue de base de données

La configuration corrompue d'une base de données peut être restaurée en réinstallant SafeGuard Management Center pour créer une nouvelle instance de la base de données, d'après les fichiers de certificat sauvegardés. Vous garantissez ainsi que tous les ordinateurs finaux SafeGuard Enterprise existants acceptent les stratégies de la nouvelle installation. Cette procédure évite de devoir configurer et restaurer de zéro l'intégralité de la base de données.

- Les certificats de l'entreprise et du responsable principal de la sécurité pour la configuration de la base de données correspondante doivent avoir été exportés sous la forme de fichiers .p12, ainsi qu'être disponibles et valides.
- Vous devez également connaître les mots de passe de ces deux fichiers .p12, ainsi que du magasin de certificats.

Procédez comme suit :

1. Installez le package d'installation de SafeGuard Management Center. Ouvrez SafeGuard Management Center. L'assistant de configuration démarre automatiquement.
2. Dans **Connexion à la base de données**, cochez la case **Créer une base de données**. Sous **Paramètres de base de données**, configurez la connexion à la base de données. Cliquez sur **Suivant**.
3. Dans **Données du responsable de la sécurité**, sélectionnez le responsable principal de la sécurité correspondant, puis cliquez sur **Importer**.

4. Cliquez sur **Importer le certificat d'authentification** pour rechercher le fichier de certificat sauvegardé. Sous **Fichier de certificat logiciel**, entrez le mot de passe de ce fichier. Cliquez sur **OK** pour confirmer.
5. Le certificat du responsable principal de la sécurité est alors importé. Cliquez sur **Suivant**.
6. Dans **Certificat d'entreprise**, cochez la case **Restaurer à l'aide d'un certificat d'entreprise existant**. Cliquez sur **Importer** pour rechercher le fichier de certificat sauvegardé qui contient le certificat d'entreprise valide. Vous êtes invité à saisir le mot de passe défini pour le magasin de certificats. Entrez le mot de passe, puis cliquez sur **OK** pour confirmer. Cliquez sur **Oui** pour confirmer le message. Le certificat d'entreprise est alors importé.
7. Cliquez sur **Suivant**, puis sur **Terminer**.

La configuration de la base de données est restaurée.

6 Licences

Vous avez besoin d'une licence valide pour utiliser SafeGuard Enterprise Management Center comme système direct. Par exemple, dans la base de données SafeGuard Enterprise, une licence valide est une condition préalable à l'envoi de stratégies aux ordinateurs finaux. Les licences de clé cryptographique appropriées sont également nécessaires à la gestion des clés cryptographiques.

Les fichiers de licence sont disponibles auprès de votre partenaire commercial. Ces fichiers doivent être importés dans la base de données SafeGuard Enterprise après l'installation. Le fichier de licence contient : des données sur le nombre de licences achetées par module/nom du propriétaire et une limite de tolérance spécifiée de dépassement du nombre de licences. Si le nombre de licences disponibles ou la limite de tolérance est dépassé, des messages d'avertissement/erreur correspondants s'affichent au démarrage de SafeGuard Management Center (voir *Licence dépassée* en page 35).

Dans la zone **Utilisateurs & ordinateurs**, SafeGuard Management Center propose une présentation de l'état de la licence du système SafeGuard Enterprise installé.
L'écran de l'état de la licence est disponible dans l'onglet **Licences** pour le nœud racine, les domaines, les unités organisationnelles, les objets conteneurs et les groupes de travail. Les responsables de la sécurité y trouveront des informations détaillées sur l'état de la licence et peuvent, s'ils disposent du droit approprié, importer des licences dans la base de données SafeGuard Enterprise.

Ce chapitre décrit le concept de licence et comment gérer les licences dans SafeGuard Management Center.

6.1 Fichier de licence

Le fichier de licence fourni pour être importé dans la base de données SafeGuard Enterprise est un fichier .XML avec une signature. Le fichier de licence inclut les informations suivantes :

- nom de la société ;
- informations supplémentaires (département, filiale par exemple) ;
- date de génération ;
- versions de SafeGuard Enterprise pour lesquelles la licence est valide ;
- nombre de licences par module ;
- informations sur la licence de la clé cryptographique ;
- date d'expiration de la licence ;
- type de licence (démonstration ou complète) ;
- signature avec certificat de signature de licence.

6.2 Licences de clé cryptographique

Pour gérer des clés cryptographiques ou des cartes à puce, les licences de clé cryptographique appropriées sont requises. Si les licences appropriées ne sont pas disponibles, il est impossible de créer de clés cryptographiques dans SafeGuard Management Center.

6.3 Licences d'évaluation et de démonstration

Le fichier de licence par défaut (licence d'évaluation) ou les fichiers de licence de démonstration individuels peuvent être utilisés pour l'évaluation ou le déploiement initial. Ces licences sont limitées dans le temps et ont une date d'expiration. Il n'existe cependant aucune restriction fonctionnelle.

Remarque : les licences d'évaluation et de démonstration ne peuvent pas être utilisées pour une utilisation directe normale.

6.3.1 Fichier de licence par défaut

Un fichier de licence par défaut est chargé automatiquement lors de l'installation de SafeGuard Enterprise Management Center. Cette licence d'évaluation (appelée licence d'évaluation de SafeGuard Enterprise) contient cinq licences pour chaque module et est limitée pour une durée de deux ans à compter de la date de publication de la version SafeGuard Enterprise concernée.

6.3.2 Fichier de licence de démonstration individuelle

Si le fichier de licence par défaut ne suffit pas à l'évaluation, vous pouvez également obtenir une licence de démonstration personnalisée en fonction de vos besoins. Dans ce cas, contactez votre partenaire commercial. L'utilisation de ce type de démonstration de licence est également limitée dans le temps. La licence est également limitée au nombre de licences par module accordé par votre partenaire commercial au cas par cas.

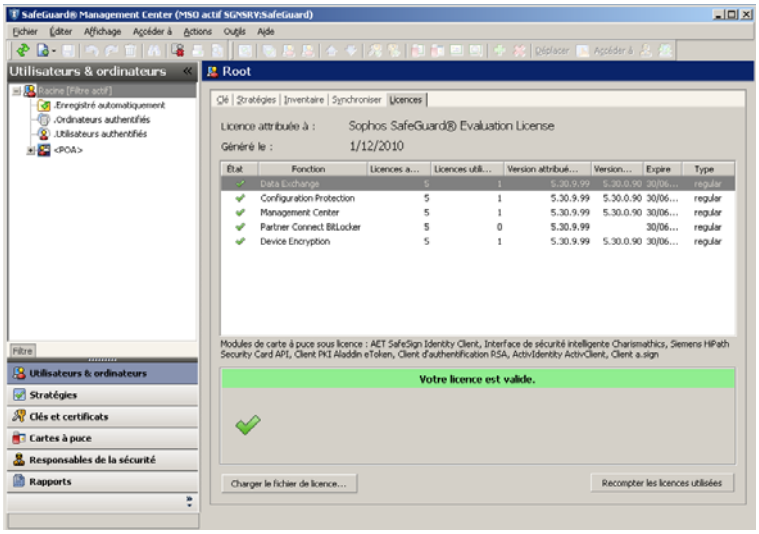
Lorsque vous démarrez SafeGuard Management Center, un message d'avertissement vous rappelle que vous utilisez des licences de démonstration. Si le nombre de licences disponibles spécifié dans la licence de démonstration est dépassé ou si la durée limite est atteinte, un message d'erreur s'affiche, voir *Licence dépassée* en page 35.

6.4 Présentation de l'état de la licence

Vous pouvez accéder à une présentation de l'état de la licence comme suit :

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs**.
2. Dans la fenêtre de navigation, à gauche, cliquez sur le nœud racine, le domaine, l'unité organisationnelle, l'objet conteneur ou le groupe de travail.
3. Dans la zone d'action, accédez à l'onglet **Licences** à droite.

L'état de la licence s'affiche.


SafeGuard® Management Center (MSO actif SGNSRV:SafeGuard)
Fichier Editer Affichage Accéder à Actions Outils Aide
Utilisateurs & ordinateurs
Root
Clé | Stratégies | Inventaire | Synchroniser | Licences
Licence attribuée à : Sophos SafeGuard® Evaluation License
Généré le : 1/12/2010
Etat Fonction Licences a... Licences utili... Version attribuée... Version... Expire Type
Data Exchange 5 1 5.30.9.99 5.30.0.90 30/06... regular
Configuration Protection 5 1 5.30.9.99 5.30.0.90 30/06... regular
Management Center 5 1 5.30.9.99 5.30.0.90 30/06... regular
Partner Connect BitLocker 5 0 5.30.9.99 30/06... regular
Device Encryption 5 1 5.30.9.99 5.30.0.90 30/06... regular
Modules de carte à puce sous licence : AET SafeSign Identity Client, Interface de sécurité intelligente Charismathics, Siemens HiPath Security Card API, Client PKI Aladdin eToken, Client d'authentification RSA, ActivIdentity ActivClient, Client a.sign
Votre licence est valide.
Charger le fichier de licence...
Recompter les licences utilisées
Utilisateurs & ordinateurs
Stratégies
Clés et certificats
Cartes à puce
Responsables de la sécurité
Rapports

L'écran est divisé en trois zones. La zone supérieure indique le nom du client pour lequel la licence a été générée ainsi que la date de génération.

La zone centrale propose des détails sur la licence. Les colonnes contiennent les détails suivants :

Colonne	Explication
État (icône)	Utilise une icône pour indiquer l'état des licences (valide, avertissement, erreur) du module concerné.
Fonction	Indique le module installé.
Licences achetées	Indique le nombre de licences achetées pour le module installé.
Licences utilisées	Indique le nombre de licences utilisées pour le module installé.

Colonne	Explication
Version attribuée la plus récente	Indique la version de SafeGuard Enterprise la plus récente pour laquelle les licences sont valides.
Version utilisée la plus récente	Indique la version de SafeGuard Enterprise installée la plus récente.
Expire	Indique la date d'expiration de la licence.
Type	Indique le type de licence : démonstration ou complète normale.
Limite de tolérance	Indique la limite de tolérance spécifiée pour le dépassement du nombre de licences achetées.

Si vous affichez l'onglet **Licences** d'un domaine/OU, la présentation indique l'état en fonction de l'ordinateur de la branche concernée.

Des détails sur les modules de clé cryptographique sous licence sont proposés sous cette présentation.

Dans la partie inférieure, un message avec une couleur d'arrière-plan en fonction du principe des feux tricolores (vert = valide, jaune = avertissement, rouge = erreur) et une icône indiquent l'état global de la licence quel que soit le domaine ou l'OU sélectionné. En cas de message d'avertissement ou d'erreur, la partie inférieure propose également des informations sur la restauration d'un état de licence valide.

Les icônes des zones centrale et inférieure ont les significations suivantes :

Licence valide

Licence non valide Avertissement

Licence non valide Erreur

Pour plus d'informations sur l'état d'une licence avec un avertissement ou une erreur, voir *Licence dépassée* en page 35.

Pour actualiser la présentation de l'état de la licence, cliquez sur **Recompter les licences utilisées**.

6.5 Importation de fichiers de licence

Condition préalable : pour importer un fichier de licence dans la base de données SafeGuard Enterprise, un responsable de la sécurité doit disposer du droit « Importer fichier de licence ».

Un fichier de licence est importé comme ci-dessous :

1. Management Center est ouvert dans la zone **Utilisateurs & ordinateurs**.
2. Dans la fenêtre de navigation, à gauche, cliquez sur le nœud racine, le domaine ou l'unité organisationnelle.
3. Dans la zone Action, accédez à l'onglet **Licences** à droite.
4. Cliquez sur le bouton **Importer fichier de licence**. Une fenêtre s'ouvre dans laquelle vous pouvez sélectionner le fichier de licence.
5. Sélectionnez le fichier de licence que vous souhaitez importer, puis cliquez sur **Ouvrir**.
6. Une présentation du contenu du nouveau fichier de licence s'affiche. Confirmez l'importation du fichier de licence.

Le fichier de licence est importé dans la base de données SafeGuard Enterprise.

Après l'importation d'un fichier de licence, les licences de module achetées sont indiquées par le type de licence **standard**. Tout module pour lequel aucune licence n'a été achetée et pour lequel la licence d'évaluation (fichier de licence par défaut) ou des licences de démonstration individuelles sont utilisées est indiqué par le type de licence **démonstration**.

Remarque : lorsqu'un nouveau fichier de licence est importé, seuls les modules inclus dans ce fichier de licence sont affectés. Toute autre information de licence de module est conservée telle que présentée dans la base de données. Ce comportement de l'importation simplifie l'évaluation ultérieure des modules supplémentaires lorsque vous achetez un ou plusieurs modules.

6.6 Licence dépassée

Une valeur de tolérance a été définie dans votre fichier de licence quant au dépassement du nombre de licences achetées et à la période de validité de la licence. Si le nombre de licences disponibles par module ou la période de validité est dépassé, un message d'avertissement s'affiche. Ceci n'affecte pas l'utilisation du système et aucune restriction n'affecte ses fonctionnalités. Vous pouvez alors réviser l'état de la licence et mettre à niveau ou renouveler votre licence. La valeur de tolérance est généralement de 10 % du nombre de licences achetées (valeur minimale : 5, valeur maximale : 5 000).

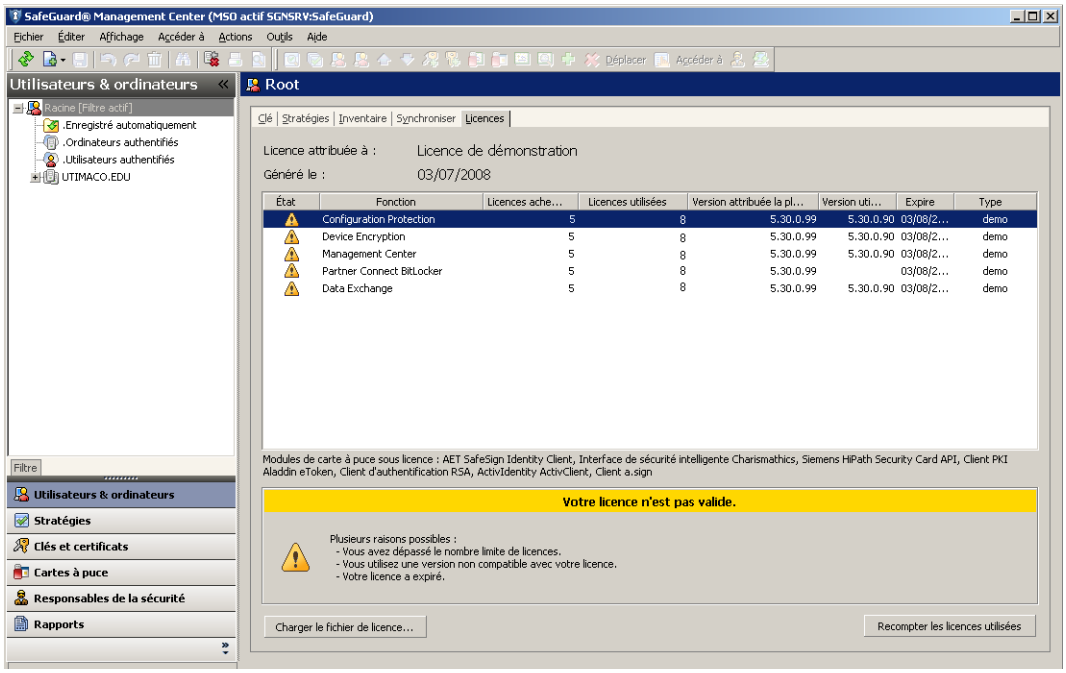
Un message d'erreur s'affiche si la valeur de tolérance est dépassée. Dans ce cas, une restriction affecte également les fonctionnalités et le déploiement de stratégies au niveau des ordinateurs finaux est désactivé. Cette désactivation ne peut pas être inversée manuellement dans SafeGuard Management Center. La licence doit être mise à niveau ou renouvelée pour pouvoir bénéficier de toutes les fonctionnalités. Outre la désactivation du déploiement de stratégies, la restriction fonctionnelle n'affecte pas les ordinateurs finaux et les stratégies déjà attribuées restent actives. Les clients peuvent également être désinstallés malgré la désactivation de la distribution de stratégies.

Les sections suivantes décrivent le comportement du système lorsque les licences sont dépassées dans les catégories Avertissement et Erreur, ainsi que l'action nécessaire pour restaurer la restriction fonctionnelle.

6.6.1 Licence non valide Avertissement

Si le nombre de licences disponibles (ou la version SafeGuard Enterprise la plus récente autorisée, par exemple en raison d'une mise à jour logicielle) est dépassé, un message d'avertissement s'affiche au démarrage de SafeGuard Management Center.

SafeGuard Management Center s'ouvre et affiche la présentation de l'état de la licence dans la zone **Utilisateurs & ordinateurs** de l'onglet **Licences**.


SafeGuard® Management Center (MSO actif SGNSRV:SafeGuard)
Fichier Éditer Affichage Accéder à Actions Outils Aide
Utilisateurs & ordinateurs
Racine [Filtre actif]
.Enregistré automatiquement
.Ordinateurs authentifiés
.Utilisateurs authentifiés
UTIMACO.EDU
Filtre
Utilisateurs & ordinateurs
Stratégies
Clés et certificats
Cartes à puce
Responsables de la sécurité
Rapports
Root
Clé | Stratégies | Inventaire | Synchroniser | Licences
Licence attribuée à : Licence de démonstration
Généré le : 03/07/2008
État Fonction Licences ache... Licences utilisées Version attribuée la pl... Version uti... Expire Type
Configuration Protection 5 8 5.30.0.99 5.30.0.90 03/08/2... demo
Device Encryption 5 8 5.30.0.99 5.30.0.90 03/08/2... demo
Management Center 5 8 5.30.0.99 5.30.0.90 03/08/2... demo
Partner Connect BitLocker 5 8 5.30.0.99 03/08/2... demo
Data Exchange 5 8 5.30.0.99 5.30.0.90 03/08/2... demo
Modules de carte à puce sous licence : AET SafeSign Identity Client, Interface de sécurité intelligente Charismathics, Siemens HiPath Security Card API, Client PKI Aladdin eToken, Client d'authentification RSA, ActivIdentity ActivClient, Client a.sign
Votre licence n'est pas valide.
Plusieurs raisons possibles :
- Vous avez dépassé le nombre limite de licences.
- Vous utilisez une version non compatible avec votre licence.
- Votre licence a expiré.
Charger le fichier de licence...
Recompter les licences utilisées

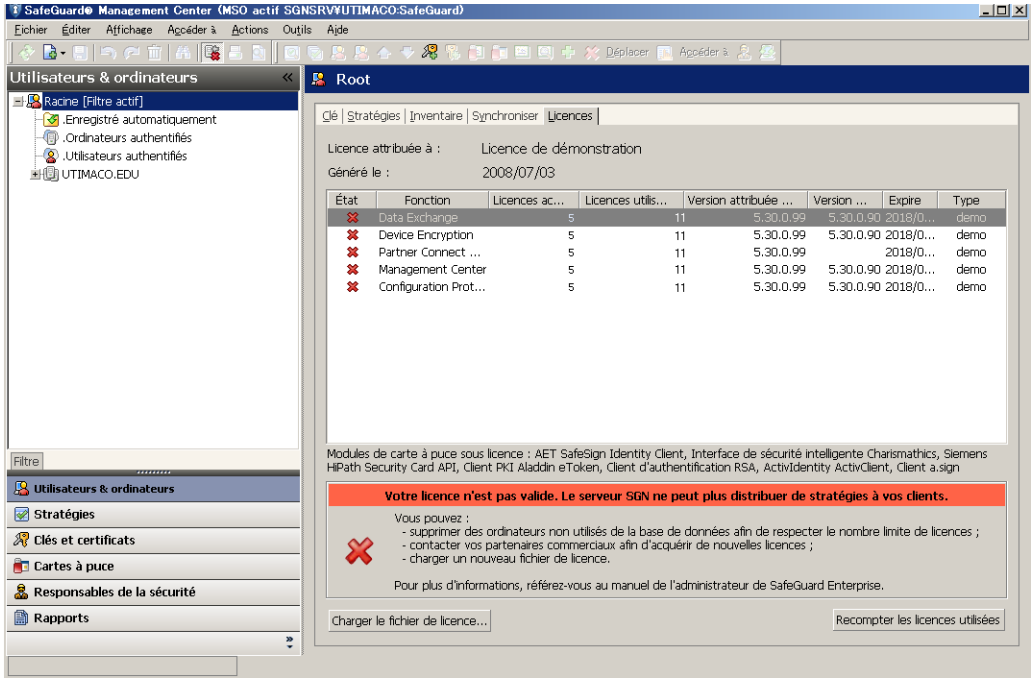
Un message d'avertissement vous informe que la licence n'est pas valide. L'utilisation des informations détaillées sur le fichier de licence vous permet de déterminer le module pour lequel le nombre de licences disponibles est dépassé. Cet état de la licence peut être restauré en faisant évoluer, en renouvelant ou en mettant la licence à niveau, voir *Licence non valide : Erreur* en page 37.

6.6.2 Licence non valide : Erreur

Si la valeur de tolérance du nombre de licences ou la période de validité définie dans la licence est dépassée, SafeGuard Management Center affiche un message d'erreur.

Le déploiement de stratégies au niveau des ordinateurs finaux est désactivé dans SafeGuard Management Center.

Un message d'erreur s'affiche également dans la zone **Utilisateurs & ordinateurs** de l'onglet **Licences**.


SafeGuard® Management Center (MSO actif SGNSRV¥UTIMACO:SafeGuard)
Fichier Éditer Affichage Accéder à Actions Outils Aide
Utilisateurs & ordinateurs
Racine [Filtre actif]
.Enregistré automatiquement
.Ordinateurs authentifiés
.Utilisateurs authentifiés
UTIMACO.EDU
Filtre
Utilisateurs & ordinateurs
Stratégies
Clés et certificats
Cartes à puce
Responsables de la sécurité
Rapports
Root
Clé | Stratégies | Inventaire | Synchroniser | Licences
Licence attribuée à : Licence de démonstration
Généré le : 2008/07/03
État Fonction Licences ac... Licences utilis... Version attribuée ... Version ... Expire Type
Data Exchange 5 11 5.30.0.99 5.30.0.90 2018/0... demo
Device Encryption 5 11 5.30.0.99 5.30.0.90 2018/0... demo
Partner Connect ... 5 11 5.30.0.99 2018/0... demo
Management Center 5 11 5.30.0.99 5.30.0.90 2018/0... demo
Configuration Prot... 5 11 5.30.0.99 5.30.0.90 2018/0... demo
Modules de carte à puce sous licence : AET SafeSign Identity Client, Interface de sécurité intelligente Charismathics, Siemens HiPath Security Card API, Client PKI Aladdin eToken, Client d'authentification RSA, ActivIdentity ActivClient, Client a.sign
Votre licence n'est pas valide. Le serveur SGN ne peut plus distribuer de stratégies à vos clients.
Vous pouvez :
- supprimer des ordinateurs non utilisés de la base de données afin de respecter le nombre limite de licences ;
- contacter vos partenaires commerciaux afin d'acquérir de nouvelles licences ;
- charger un nouveau fichier de licence.
Pour plus d'informations, référez-vous au manuel de l'administrateur de SafeGuard Enterprise.
Charger le fichier de licence...
Recompter les licences utilisées

L'utilisation des informations détaillées sur le fichier de licence vous permet de déterminer le module pour lequel le nombre de licences disponibles est dépassé.

Les options suivantes s'offrent à vous pour inverser la restriction de la fonctionnalité :

- Redistribuer des licences

  Pour disposer d'un nombre suffisant de licences disponibles, vous pouvez désinstaller le logiciel sur les ordinateurs non utilisés et supprimer ainsi les ordinateurs de la base de données SafeGuard Enterprise.

- Mettre à niveau/renouveler des licences

  Contactez votre partenaire commercial pour mettre à niveau ou renouveler votre licence. Un nouveau fichier de licence à importer dans la base de données SafeGuard Enterprise vous sera fourni.

- Importer un nouveau fichier de licence

  Si vous avez renouvelé ou mis à niveau votre licence, vous pouvez importer le fichier de licence reçu dans la base de données SafeGuard Enterprise. Le nouveau fichier importé remplace le fichier de licence non valide.

Lorsque vous redistribuez des licences ou que vous importez un fichier de licence valide, la restriction fonctionnelle est annulée et le système fonctionne normalement.

7 Responsables de la sécurité de SafeGuard Enterprise

SafeGuard Enterprise peut être administré par un ou plusieurs responsables de la sécurité. La gestion basée sur le rôle de SafeGuard Enterprise permet de répartir l'administration entre plusieurs utilisateurs. Un utilisateur peut se voir attribuer un ou plusieurs rôles. Afin d'améliorer la sécurité, une autorisation supplémentaire d'action peut être attribuée au rôle d'un responsable.

Administrateur de niveau supérieur, le responsable principal de la sécurité (MSO, Master Security Officer), possédant tous les droits et un certificat qui n'expire pas, est créé par défaut au cours de la configuration initiale de SafeGuard Management Center. D'autres responsables de la sécurité peuvent alors être attribués à des tâches spécifiques, comme le support ou l'audit.

À titre pratique, vous pouvez organiser les responsables de la sécurité de manière hiérarchique dans la zone de navigation de SafeGuard Management Center et ce, afin de représenter la structure organisationnelle de votre société. Toutefois, cette hiérarchie ne tient pas compte des droits et des rôles.

7.1 Rôles du responsable de la sécurité

Pour plus de simplicité, SafeGuard Enterprise propose des rôles prédéfinis pour les responsables de la sécurité dotés de diverses fonctions. Un responsable de la sécurité possédant les droits nécessaires peut également définir de nouveaux rôles à partir d'une liste d'actions/de droits et les attribuer à des responsables de la sécurité particuliers.

Les types de rôle suivants sont fournis :

- Rôle du responsable principal de la sécurité
- Rôles prédéfinis
- Rôles personnalisés

7.1.1 Responsable principal de la sécurité

Après avoir installé SafeGuard Enterprise, un responsable principal de la sécurité (MSO, Master Security Officer) est créé par défaut au cours de la configuration initiale de SafeGuard Management Center. Le responsable principal de la sécurité est un responsable de la sécurité de niveau supérieur. Il bénéficie de tous les droits et peut accéder à tous les objets. À ce titre, il peut être comparé à un administrateur Windows. Les droits du responsable principal de la sécurité ne peuvent pas être modifiés.

Plusieurs responsables principaux de la sécurité peuvent être créés pour une seule instance de SafeGuard Management Center. Pour des raisons de sécurité, la création d'au moins un MSO supplémentaire est fortement recommandée. Les MSO supplémentaires peuvent être supprimés.

Toutefois, il doit toujours rester un utilisateur bénéficiant du rôle de MSO et créé de manière explicite en tant que MSO dans la base de données SafeGuard Enterprise.

Un responsable principal de la sécurité peut déléguer des tâches à une autre personne. Pour ce faire, vous pouvez procéder de deux façons :

- Un nouveau responsable de la sécurité peut être créé dans **Responsables de la sécurité**.
- Un utilisateur ou tous les membres d'un conteneur importé d'Active Directory et visibles dans le répertoire racine de SafeGuard Management Center peuvent être promus au rang de responsable de la sécurité dans **Utilisateurs et ordinateurs**.

Un ou plusieurs rôles peuvent alors être attribués aux responsables de la sécurité. Par exemple, un utilisateur peut se voir attribuer le rôle de responsable supervision et celui de responsable support.

Toutefois, le responsable principal de la sécurité peut également créer des rôles personnalisés et les attribuer à des utilisateurs particuliers.

7.1.2 Rôles prédéfinis

Dans SafeGuard Management Center, les rôles de responsable de la sécurité suivants, sauf ceux du MSO, sont prédéfinis. L'attribution des droits à ces rôles prédéfinis ne peut être changée. Par exemple, si un rôle prédéfini possède le droit de « création d'éléments de stratégie et de groupes de stratégies », ce droit ne peut pas être supprimé du rôle. De même, un nouveau droit ne peut pas être ajouté à un rôle prédéfini. Toutefois, vous pouvez attribuer à tout moment une authentification responsable à des rôles prédéfinis.

- **Responsable supervision**

  Les responsables supervision peuvent accéder à leurs propres nœuds dans la zone Responsable de la sécurité. De même, ils sont autorisés à gérer les responsables de la sécurité inclus dans leurs nœuds respectifs.

- **Responsable de la sécurité**

  Les responsables de la sécurité possèdent des droits étendus, y compris des droits de configuration de SafeGuard Enterprise, de gestion des stratégies et des clés, ainsi que des autorisations relatives au contrôle et à la récupération.

- **Responsable support**

  Les responsables support ont le droit d'effectuer des actions de récupération. Ils peuvent également afficher la plupart des zones de fonctions de SafeGuard Management Center.

- **Responsable audit**

  Pour contrôle SafeGuard Enterprise, les responsables audit peuvent afficher la plupart des zones de fonctions de SafeGuard Management Center.

- **Responsable récupération**

  Les responsables récupération ont le droit de réparer la base de données SafeGuard Enterprise.

7.1.3 Rôles personnalisés

En tant que responsable de la sécurité possédant les droits nécessaires, vous pouvez définir de nouveaux rôles à partir d'une liste d'actions/de droits, puis les attribuer à un responsable de la sécurité existant ou nouveau. De même qu'avec les rôles prédéfinis, vous pouvez activer l'authentification responsable supplémentaire pour une fonction du rôle à tout moment.

Lors de l'attribution d'un nouveau rôle, notez les informations suivantes relatives à l'authentification supplémentaire :

Avis : Si un utilisateur a deux rôles avec les mêmes droits attribués et si l'authentification supplémentaire est attribuée à l'un des rôles, elle s'applique automatiquement à l'autre également.

Un responsable de la sécurité bénéficiant des droits nécessaires peut ajouter des droits à un rôle personnalisé, ou en supprimer. Contrairement aux rôles prédéfinis, les rôles personnalisés peuvent être modifiés et même supprimés le cas échéant. Lorsque vous supprimez le rôle, il n'est plus attribué à aucun utilisateur. Si un seul rôle est attribué à un utilisateur et si ce rôle est supprimé, l'utilisateur ne peut plus se connecter à SafeGuard Management Center.

Le rôle et les actions définies dans le cadre de celui-ci déterminent ce qu'un utilisateur peut faire et ne pas faire. Ceci est également vrai si l'utilisateur a plusieurs rôles. Lorsque l'utilisateur s'est connecté à Management Center, les seules zones qui sont activées et affichées sont celles qui sont nécessaires pour son rôle. Ceci s'applique également aux zones des scripts et de l'API. Il est donc important de toujours activer l'affichage de la zone dans laquelle les actions respectives sont définies. Les actions sont triées par zone de fonctions et sont disposées de manière hiérarchique. Cette structure permet de visualiser les actions nécessaires à l'exécution d'autres actions.

7.1.4 Authentification responsable supplémentaire

Une authentification responsable supplémentaire (également appelée « règle des deux personnes ») peut être attribuée à des actions spécifiques d'un rôle. Cela signifie que l'utilisateur de ce rôle n'est autorisé à effectuer qu'une certaine action si un utilisateur d'un autre rôle est présent et confirme l'exécution de cette action.

Vous pouvez attribuer une authentification supplémentaire indifféremment à des rôles prédéfinis ou personnalisés. Dès que deux responsables minimum ont le même rôle, le rôle personnalisé peut également être sélectionné.

Le rôle consistant à effectuer l'autorisation supplémentaire doit être préalablement attribué à un utilisateur. De plus, la base de données SafeGuard Enterprise doit compter au moins deux responsables de la sécurité. Lorsqu'une action requiert une authentification supplémentaire, celle-ci est nécessaire même si l'utilisateur détient un autre rôle ne nécessitant pas d'authentification supplémentaire pour la même action.

Si un responsable crée un rôle alors qu'il ne possède pas le droit de modification de l'authentification supplémentaire, les paramètres relatifs à une authentification supplémentaire du nouveau rôle seront prérenseignés afin de correspondre à ceux définis pour le responsable de la création de ce rôle.

Remarque : Deux responsables de la sécurité ne doivent pas utiliser le même compte Windows sur le même PC. Dans le cas contraire, il est impossible de distinguer correctement leurs droits d'accès. Une authentification supplémentaire ne peut être utile que lorsque les responsables de la sécurité doivent s'authentifier à l'aide de clés cryptographiques/cartes à puce.

7.2 Création d'un rôle

Condition préalable : pour créer un rôle, vous devez posséder le droit d'affichage et de création de rôles de responsable de la sécurité. Pour attribuer des authentifications supplémentaires, vous devez posséder le droit de « modification des paramètres d'authentification supplémentaire ».

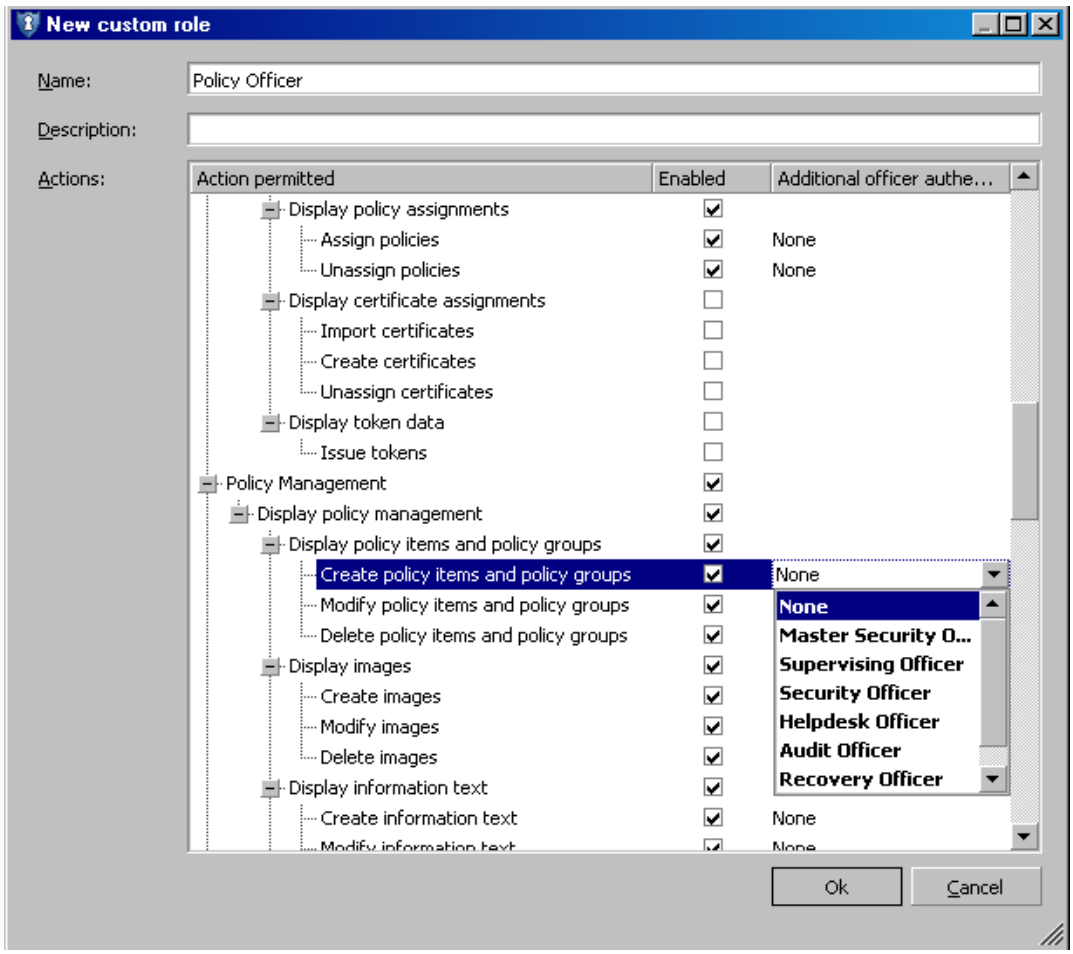
Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Cliquez avec le bouton droit sur **Rôles personnalisés** et sélectionnez **Nouveau** > **Nouveau rôle personnalisé**.
3. Dans le champ **Nouveau rôle personnalisé**, entrez un nom et une description pour le rôle.
4. Attribuez les actions à ce rôle : Cochez les cases en regard de l'action requise dans la colonne **Active**. Les actions sont triées par zone de fonctions et sont disposées de manière hiérarchique. Cette structure permet de visualiser les actions nécessaires à l'exécution d'autres actions.

5. Si nécessaire, attribuez une **authentification responsable supplémentaire** : Cliquez sur le paramètre par défaut **Aucune** et, depuis la liste, sélectionnez le rôle requis. Si un responsable crée un rôle sans posséder de droit de modification de l'authentification supplémentaire, les paramètres relatifs à l'authentification supplémentaire seront prérenseignés en fonction de l'authentification supplémentaire définie pour les rôles du responsable. Vous pouvez sélectionner une authentification supplémentaire si celle-ci a été définie pour plusieurs rôles du responsable.

6. Cliquez sur **OK**.

Le nouveau rôle est affiché sous **Rôles personnalisés** dans la fenêtre de navigation. Lorsque vous cliquez sur le rôle, les actions autorisées sont affichées dans la zone d'action de droite.



7.3 Attribution d'un rôle à un responsable de la sécurité

Condition préalable : pour attribuer un rôle, vous devez posséder le droit d'affichage et de modification des responsables de la sécurité.

Procédez comme suit :

1. Sélectionnez le responsable approprié dans la fenêtre de navigation. Les propriétés s'affichent dans la zone d'action de droite.
2. Attribuez les rôles nécessaires en cochant les cases correspondantes en regard des rôles disponibles. Les rôles prédéfinis s'affichent en gras.
3. Cliquez sur le symbole à double flèche d'**actualisation** dans la barre d'outils.

Le rôle est attribué au responsable de la sécurité.

7.4 Affichage des propriétés du responsable et du rôle

Condition préalable : pour obtenir un aperçu des propriétés du responsable ou de l'attribution du rôle, vous devez posséder le droit d'affichage des responsables de la sécurité et des rôles de ces derniers.

Procédez comme suit :

1. Dans SafeGuard Management Center, cliquez sur **Responsables de la sécurité**.
2. Dans la zone de navigation de gauche, double-cliquez sur l'objet dont vous souhaitez obtenir un aperçu.

Les informations disponibles dans la zone d'action de droite sont fonction de l'objet sélectionné.

7.4.1 Afficher les propriétés de MSO

Les informations générales et de modification relatives au MSO s'affichent.

7.4.2 Afficher les propriétés des responsables de la sécurité

Les informations générales et de modification relatives au responsable de la sécurité s'affichent.

1. Dans **Propriétés**, sélectionnez l'onglet **Actions** afin d'afficher un résumé des actions autorisées et des rôles attribués au responsable de la sécurité.

7.4.3 Afficher les droits et les rôles des responsables de la sécurité

Un résumé des actions de tous les rôles attribués au responsable de la sécurité s'affiche. L'arborescence permet de visualiser les actions nécessaires à l'exécution d'autres actions. Les rôles attribués peuvent également être affichés.

1. Dans **Actions**, sélectionnez une action afin d'afficher tous les rôles attribués contenant cette action.
2. Double-cliquez sur un rôle pour fermer la boîte de dialogue **Propriétés**, puis afficher les propriétés du rôle.

7.4.4 Afficher les propriétés du rôle

Les informations générales et de modification relatives au rôle s'affichent.

1. Dans **Propriétés**, sélectionnez l'onglet **Attribution** afin d'afficher les responsables de la sécurité attribués à ce rôle.

7.4.5 Afficher l'attribution du rôle

1. Dans **Attribution**, double-cliquez sur un responsable de la sécurité afin de fermer la boîte de dialogue **Propriétés**, puis d'afficher les données générales et les rôles du responsable de la sécurité.

7.5 Modification d'un rôle

Procédez comme suit :

- Modifier l'authentification supplémentaire uniquement.
- Modifier toutes les propriétés du rôle.

L'icône en regard des rôles affiche l'action disponible :

Icône	Description
	Le rôle peut être modifié (ajouter/supprimer des actions).
	L'authentification supplémentaire peut être modifiée.
	Les deux types de modification sont disponibles.

Avis : vous ne pouvez pas modifier les rôles prédéfinis et les actions qui leur sont attribuées. Si une authentification supplémentaire est activée, celle-ci peut être modifiée pour tous les rôles, même les rôles prédéfinis.

7.5.1 Modifier l'authentification supplémentaire uniquement

Condition préalable : pour attribuer une authentification supplémentaire, vous devez posséder le droit d'affichage des rôles du responsable de la sécurité et de « modification des paramètres d'authentification supplémentaire ».

Procédez comme suit :

1. Dans Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, sous **Rôles personnalisés**, cliquez sur le rôle à modifier. Dans la zone d'action de droite, cliquez sur le paramètre requis dans la colonne **Authentification responsable supplémentaire** et sélectionnez un rôle différent à partir de la liste. Les rôles prédéfinis s'affichent en gras.
3. Pour enregistrer vos modifications apportées à la base de données, cliquez sur l'icône **Enregistrer** de la barre d'outils.

L'authentification responsable supplémentaire a été modifiée pour ce rôle.

7.5.2 Modifier toutes les propriétés d'un rôle

Condition préalable : pour modifier un rôle personnalisé, vous devez posséder le droit d'affichage et de modification des rôles de responsable de la sécurité. Pour réattribuer une authentification supplémentaire, vous devez posséder le droit de « modification des paramètres d'authentification supplémentaire ».

Procédez comme suit :

1. Dans Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, sous **Rôles personnalisés**, cliquez avec le bouton droit sur le rôle à modifier et sélectionnez **Modifier des rôles de responsable de la sécurité**.
3. Modifiez les propriétés selon vos besoins. Modifiez les propriétés d'authentification supplémentaire en cliquant sur la valeur de cette colonne et en sélectionnant le rôle requis.
4. Pour enregistrer vos modifications apportées à la base de données, cliquez sur l'icône **Enregistrer** de la barre d'outils.

Le rôle a été modifié.

7.6 Copie d'un rôle

Pour créer un rôle dont les propriétés sont identiques à celles d'un rôle existant, vous pouvez utiliser le rôle existant comme modèle pour le nouveau rôle. Vous pouvez sélectionner un rôle prédéfini ou personnalisé comme modèle.

Condition préalable : vous pouvez utiliser des rôles existants comme modèles uniquement si le responsable de la sécurité actuellement authentifié possède tous les droits contenus dans le modèle de rôle spécifique. Par conséquent, cette fonction peut ne pas être disponible pour les responsables ne possédant qu'un nombre d'actions limité.

Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le rôle à copier et sélectionnez **Nouveau** > **Nouvelle copie du rôle**. Dans **Nouveau rôle personnalisé**, toutes les propriétés du rôle existant sont présélectionnées à l'avance.
3. Entrez un nouveau nom pour ce rôle et modifiez les propriétés selon les besoins.
4. Pour enregistrer vos modifications apportées à la base de données, cliquez sur l'icône **Enregistrer** de la barre d'outils.

Le nouveau rôle est créé.

7.7 Suppression d'un rôle

Avis : vous ne pouvez pas supprimer des rôles prédéfinis.

Condition préalable : pour supprimer un rôle, vous devez posséder le droit d'affichage et de suppression des rôles de responsable de la sécurité.

Procédez comme suit :

1. Dans Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, sous **Rôles personnalisés**, cliquez avec le bouton droit sur le rôle à supprimer et sélectionnez **Supprimer**. En fonction des propriétés du rôle, un message d'avertissement spécifique s'affichera.

   Avis : lorsque vous supprimez un rôle, tous les responsables de la sécurité auxquels ce rôle est attribué perdent ce dernier. Si le rôle est le seul attribué à un responsable de la sécurité, ce dernier ne sera plus en mesure de se connecter à SafeGuard Management Center, sauf s'il se voit attribuer un nouveau rôle par un responsable de la sécurité supérieur.

Si le rôle est utilisé à des fins d'authentification supplémentaire, le MSO devra effectuer une authentification supplémentaire.

3. Confirmez la suppression en cliquant sur **Oui**.
4. Pour enregistrer vos modifications apportées à la base de données, cliquez sur l'icône **Enregistrer** de la barre d'outils.

Le rôle est supprimé de la fenêtre de navigation et de la base de données.

7.8 Création d'un responsable principal de la sécurité

Condition préalable : pour créer un responsable principal de la sécurité, vous devez posséder le droit d'affichage et de création de responsables de la sécurité.

Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le nœud **Responsables principaux de la sécurité** et sélectionnez **Nouveau** > **Nouveau responsable de la sécurité**.
3. Procédez de la façon suivante dans la boîte de dialogue **Nouveau responsable principal de la sécurité** :

Champ/case à cocher	Description
Activé	Le responsable peut être désactivé jusqu'à nouvel avis. Le responsable est dans le système mais ne peut pas encore se connecter à SafeGuard Management Center. Il ne peut le faire et effectuer ses tâches d'administration que lorsqu'un autre responsable l'active.
Nom	Entrez le nom du responsable tel qu'indiqué dans les certificats créés par SafeGuard Enterprise sous la forme cn =. Le responsable est également affiché sous ce nom dans la fenêtre de navigation de Management Center. Ce nom doit être unique. Valeur maximale : 256 caractères
Description	Facultatif Valeur maximale : 256 caractères
Téléphone portable	Facultatif Valeur maximale : 128 caractères
E-mail	Facultatif Valeur maximale : 256 caractères

Champ/case à cocher	Description
Connexion sur la clé cryptographique	La connexion peut s'effectuer de la façon suivante : **(Pas de carte à puce)** Le responsable ne peut pas se connecter avec une clé cryptographique. Il doit se connecter en saisissant les informations de connexion (nom d'utilisateur/mot de passe). **(Facultatif)** La connexion peut s'effectuer avec une clé cryptographique ou en saisissant les informations de connexion. Le responsable de la sécurité a le choix. **(Obligatoire)** Une clé cryptographique doit être utilisée pour la connexion. Pour ce faire, la clé privée appartenant au certificat du responsable de la sécurité doit se trouver sur la clé cryptographique.
Certificat	Un responsable a toujours besoin d'un certificat pour se connecter à Management Center. Le certificat peut être créé par SafeGuard Enterprise lui-même ou un certificat existant peut être utilisé. Si la connexion avec une clé cryptographique est essentielle, le certificat doit être ajouté à la clé cryptographique du responsable. **Créer :** Le certificat et le fichier de clés sont créés et enregistrés dans un emplacement choisi. Entrez et confirmez le mot de passe du fichier de clés .p12. Le fichier .p12 doit être à la disposition du responsable lorsqu'il se connecte. Le certificat créé est attribué automatiquement au responsable et affiché dans **Certificat**. Si des règles de mot de passe de SafeGuard Enterprise sont utilisées, celles-ci doivent être désactivées dans Active Directory. **Avis** : Longueur max. du chemin d'enregistrement et du nom de fichier : 260 caractères. Lors de la création d'un responsable de la sécurité, la partie publique du certificat suffit. Lors de la connexion à Management Center, cependant, la partie privée du certificat (le fichier de clés) est également requise. Si elle n'est pas disponible dans la base de données, elle doit l'être pour le responsable de la sécurité (sur une carte mémoire par exemple), et peut être stockée dans le magasin de certificats pendant la connexion.
Certificat	**Importation :** Un certificat existant est utilisé et attribué au responsable lors de l'importation. Si l'importation s'effectue à partir d'un fichier de clés .p12, le mot de passe du certificat doit être connu. Si un conteneur de certificats PKCS#12 est sélectionné, tous les certificats sont chargés dans la liste de certificats attribuables. L'attribution du certificat s'effectue après l'importation, en le sélectionnant dans la liste déroulante.

4. Pour confirmer, cliquez sur **OK**.

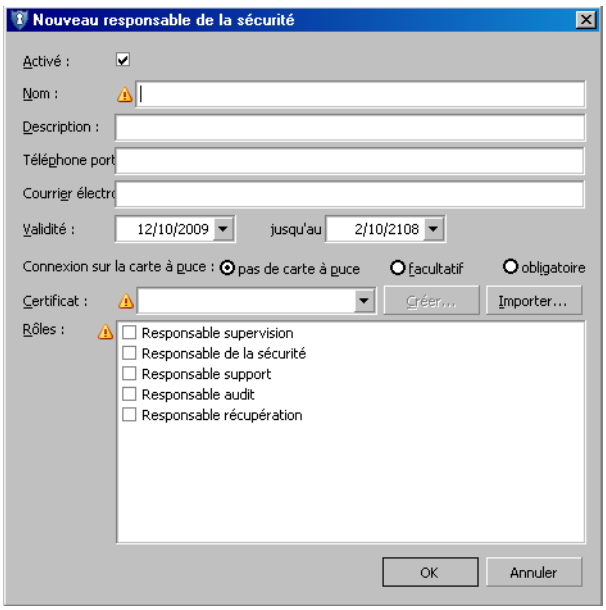
Le nouveau responsable principal de la sécurité s'affiche dans la fenêtre de navigation, sous le nœud **Responsables principaux de la sécurité**. Leurs propriétés peuvent être affichées en sélectionnant le responsable concerné dans la fenêtre de navigation. Le MSO peut se connecter à SafeGuard Management Center avec le nom affiché.

7.9 Création d'un responsable de la sécurité

Condition préalable : pour créer un responsable de la sécurité, vous devez posséder le droit d'affichage et de création de responsables de la sécurité.

Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le nœud du responsable de la sécurité où vous souhaitez placer le nouveau responsable de la sécurité, puis sélectionnez **Nouveau** > **Nouveau responsable de la sécurité**.
3. Procédez de la façon suivante dans la boîte de dialogue **Nouveau responsable de la sécurité** :



Champ/case à cocher	Description
Activé	Le responsable peut être désactivé jusqu'à nouvel avis. Le responsable est dans le système mais ne peut pas encore se connecter à SafeGuard Management Center. Il ne peut le faire et effectuer ses tâches d'administration que lorsqu'un autre responsable l'active.
Nom	Entrez le nom du responsable tel qu'indiqué dans les certificats créés par SafeGuard Enterprise sous la forme cn =. Le responsable est également affiché sous ce nom dans la fenêtre de navigation de Management Center. Ce nom doit être unique. Valeur maximale : 256 caractères
Description	Facultatif Valeur maximale : 256 caractères
Téléphone portable	Facultatif Valeur maximale : 128 caractères
E-mail	Facultatif Valeur maximale : 256 caractères
Validité	Sélectionnez les dates de début et de fin d'autorisation de connexion du responsable à Management Center.
Connexion sur la clé cryptographique	La connexion peut s'effectuer de la façon suivante : (**Pas de carte à puce**) Le responsable ne peut pas se connecter avec une clé cryptographique. Il doit se connecter en saisissant ses informations de connexion (nom d'utilisateur/mot de passe). (**Facultatif**) La connexion peut s'effectuer avec une clé cryptographique ou en saisissant les informations de connexion. Le responsable de la sécurité a le choix. (**Obligatoire**) Une clé cryptographique doit être utilisée pour la connexion. Pour ce faire, la clé privée appartenant au certificat du responsable de la sécurité doit se trouver sur la clé cryptographique.

Champ/case à cocher	Description
Certificat	Un responsable a toujours besoin d'un certificat pour se connecter à Management Center. Le certificat peut être créé par SafeGuard Enterprise lui-même ou un certificat existant peut être utilisé. Si la connexion avec une clé cryptographique est essentielle, le certificat doit être ajouté à la clé cryptographique du responsable. **Créer :** Le certificat et le fichier de clés sont créés et enregistrés dans un emplacement choisi. Entrez et confirmez le mot de passe du fichier de clés .p12. Le fichier .p12 doit être à la disposition du responsable lorsqu'il se connecte. Le certificat créé est attribué automatiquement au responsable et affiché dans **Certificat**. Si des règles de mot de passe de SafeGuard Enterprise sont utilisées, celles-ci doivent être désactivées dans Active Directory. **Avis** : Longueur max. du chemin d'enregistrement et du nom de fichier : 260 caractères. Lors de la création d'un responsable de la sécurité, la partie publique du certificat suffit. Lors de la connexion à Management Center, cependant, la partie privée du certificat (le fichier de clés) est également requise. Si elle n'est pas disponible dans la base de données, elle doit l'être pour le responsable de la sécurité (sur une carte mémoire par exemple), et peut être stockée dans le magasin de certificats pendant la connexion.
Certificat	**Importation :** Un certificat existant est utilisé et attribué au responsable lors de l'importation. Si l'importation s'effectue à partir d'un fichier de clés .p12, le mot de passe du certificat doit être connu. Si un conteneur de certificats PKCS#12 est sélectionné, tous les certificats sont chargés dans la liste de certificats attribuables. L'attribution du certificat s'effectue après l'importation, en le sélectionnant dans la liste déroulante.
Rôles du responsable de la sécurité	**Rôles** Des rôles prédéfinis ou personnalisés peuvent être attribués au responsable. Les droits associés à chaque rôle s'affichent soit en cliquant sur le rôle concerné sous **Action autorisée** dans la zone d'action, soit en cliquant avec le bouton droit sur le responsable et en sélectionnant **Propriétés, Actions**. Il est possible d'attribuer plusieurs rôles à un utilisateur. Les rôles prédéfinis s'affichent en gras. L'exécution d'une authentification supplémentaire est expressément liée au fait de détenir un rôle particulier.

4. Pour confirmer, cliquez sur **OK**.

Le nouveau responsable de la sécurité s'affiche dans la fenêtre de navigation, sous le nœud **Responsables de la sécurité** respectif. Leurs propriétés peuvent être affichées en sélectionnant le responsable concerné dans la fenêtre de navigation. Le responsable de la sécurité peut se connecter à SafeGuard Management Center avec le nom affiché. Vous devez ensuite attribuer les objets/domaines de répertoire au responsable afin que celui-ci puisse exécuter ses tâches.

7.10 Attribution d'objets de répertoire à un responsable de la sécurité

Afin que le responsable de la sécurité puisse exécuter ses tâches, il doit posséder les droits d'accès aux objets de répertoire. L'accès peut être autorisé aux nœuds de domaine et de groupe de travail, ainsi qu'au nœud « .Autoregistered » situé sous le répertoire racine.

Condition préalable : pour attribuer des objets de répertoire à un responsable, vous devez posséder les droits d'utilisateurs et d'ordinateurs « d'affichage des droits d'accès des responsables de la sécurité » et « d'autoriser/de refuser l'accès au répertoire ».

Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, sélectionnez les objets de répertoire requis.
3. Dans la zone d'action de droite, cliquez sur l'onglet **Accès**.
4. Pour attribuer les droits pour les objets sélectionnés, faites glisser le responsable requis depuis l'extrémité droite au tableau **Accès**. Pour annuler l'attribution, faites glisser le responsable de la sécurité dans le tableau **Responsables**.
5. Pour enregistrer les modifications apportées à la base de données, cliquez sur l'icône **Enregistrer** de la barre d'outils.

Les objets sélectionnés sont disponibles pour le responsable de la sécurité sélectionné.

7.11 Promotion de responsables de la sécurité

Procédez comme suit :

- promouvoir un utilisateur au rang de responsable de la sécurité dans la zone **Utilisateurs et ordinateurs**
- promouvoir un responsable de la sécurité au rang de responsable principal de la sécurité dans la zone **Responsables de la sécurité**

7.11.1 Conditions préalables à la promotion d'un utilisateur

Un responsable de la sécurité possédant les droits nécessaires peut promouvoir des utilisateurs au rang de responsable de la sécurité et leur attribuer des rôles.

Les responsables de la sécurité ainsi créés peuvent se connecter à SafeGuard Management Center avec leurs informations d'identification Windows ou leur code PIN de clé cryptographique/carte à puce. Ils peuvent travailler et être gérés comme tout autre responsable de la sécurité.

Les conditions préalables suivantes doivent être remplies :

- L'utilisateur à promouvoir doit avoir été importé d'un Active Directory et visible dans la zone **Utilisateurs et ordinateurs** de SafeGuard Management Center.
- Pour qu'un utilisateur promu puisse se connecter à SafeGuard Management Center en tant que responsable de la sécurité, vous devez avoir préalablement créé ou importé un certificat utilisateur, puis attribué celui-ci à l'utilisateur. Pour rendre possible la connexion avec les informations d'identification Windows, le fichier .p12 contenant la clé privée doit se trouver dans la base de données SafeGuard Enterprise. Pour se connecter avec un code PIN de clé cryptographique ou de carte à puce, le fichier .p12 contenant la clé privée doit se trouver sur la clé cryptographique ou la carte à puce.

7.11.2 Promouvoir un utilisateur au rang de responsable de la sécurité

Condition préalable : pour promouvoir un utilisateur, vous devez être responsable principal de la sécurité.

Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Utilisateurs & ordinateurs**.
2. Sélectionnez l'utilisateur à promouvoir et cliquez sur l'onglet **Certificat** dans la zone d'action de droite.
   - Si un certificat a été attribué à l'utilisateur, il s'affiche dans la zone d'action.
   - Si aucun certificat n'a encore été attribué à l'utilisateur, attribuez un certificat en cliquant sur l'icône **Importer un certificat** de la barre d'outils. Repérez les fichiers de magasin de certificats requis (*.cer) et de clé privée (*.p12), puis cliquez sur **OK**.
3. Cliquez avec le bouton droit sur l'utilisateur que vous souhaitez promouvoir au rang de responsable de la sécurité et sélectionnez **Faire de cet utilisateur un responsable**.
4. Activez les rôles requis dans **Sélectionner les rôles** et confirmez en cliquant sur **OK**.

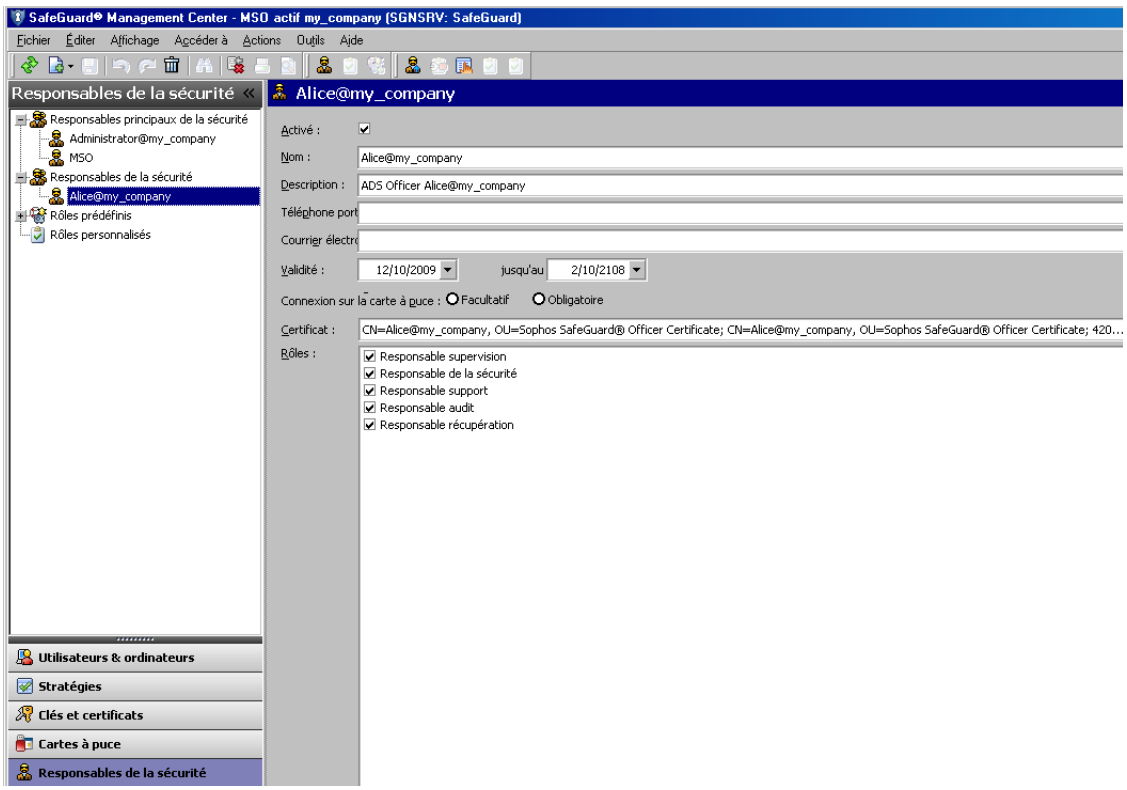
   Les rôles prédéfinis s'affichent en gras. Si un responsable enfant s'est vu attribuer davantage de rôles que le responsable connecté, les rôles supplémentaires s'affichent en italique.

5. Pour enregistrer les modifications apportées à la base de données, cliquez sur l'icône **Enregistrer** de la barre d'outils.

L'utilisateur est désormais promu et s'affiche dans la zone **Responsables de la sécurité** avec son nom d'utilisateur. Leurs propriétés peuvent être affichées en sélectionnant le responsable concerné dans la fenêtre de navigation. La clé privée de l'utilisateur est stockée dans la base de données et l'option **Pas de carte à puce** est activée. L'option **Facultatif** est activée si la clé privée de l'utilisateur réside sur la clé cryptographique ou la carte à puce.

Si nécessaire, vous pouvez faire glisser le responsable de la sécurité *à la position requise dans l'arborescence **Responsables de la sécurité**.

Le responsable de la sécurité peut se connecter à SafeGuard Management Center avec le nom affiché.



7.11.3 Promotion d'un responsable de la sécurité au rang de responsable principal de la sécurité

Condition préalable : pour promouvoir un responsable de la sécurité, vous devez posséder le droit d'affichage et de modification de responsables de la sécurité.

Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le responsable de la sécurité à promouvoir et sélectionnez **Promouvoir au rang de responsable principal de la sécurité**.
3. Si le responsable promu possède des enfants, vous êtes invité à sélectionner un nouveau nœud parent pour les enfants.

Le responsable de la sécurité a été promu et s'affiche sous le nœud **Responsables principaux de la sécurité**. En tant que responsable principal de la sécurité, le responsable promu recevra tous les droits sur l'ensemble des objets. Par conséquent, il perdra tous les droits attribués ainsi que l'accès au domaine autorisé de manière individuelle dans **Utilisateur et ordinateurs**.

7.12 Rétrogradation de responsables principaux de la sécurité

Condition préalable : pour rétrograder des responsables principaux de la sécurité au rang de responsable de la sécurité, vous devez être responsable principal de la sécurité.

Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le responsable principal de la sécurité à rétrograder et sélectionnez **Rétrograder au rang de responsable de la sécurité**.
3. Vous êtes invité à sélectionner un nœud parent pour le responsable et d'attribuer à ce dernier au moins un rôle.

Le responsable de la sécurité a été rétrogradé et s'affiche sous le nœud **Responsables de la sécurité** sélectionné. Le responsable ainsi rétrogradé perdra tous ses droits sur l'ensemble des objets et ne recevra que ceux attribués à son ou ses rôles. Un responsable rétrogradé ne possède aucun droit sur les domaines. Vous devez accorder individuellement des droits d'accès dans la zone **Utilisateurs et ordinateurs**, sous l'onglet **Accès**.

7.13 Modification du certificat de responsable de la sécurité

Condition préalable : pour modifier le certificat d'un responsable de la sécurité ou d'un responsable principal de la sécurité, vous devez posséder le droit d'affichage et de modification de responsables de la sécurité.

Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le responsable de la sécurité dont vous souhaitez modifier le certificat. Le certificat actuellement attribué s'affiche dans la zone d'action de droite, située sous **Certificats**.
3. Dans la zone d'action, cliquez sur la liste déroulante **Certificats** et sélectionnez un certificat différent.
4. Pour enregistrer les modifications apportées à la base de données, cliquez sur l'icône **Enregistrer** de la barre d'outils.

7.14 Organisation des responsables de la sécurité dans l'arborescence

À titre pratique, vous pouvez organiser les responsables de la sécurité de manière hiérarchique dans la fenêtre de navigation **Responsables de la sécurité** et ce, afin de représenter la structure organisationnelle de votre société.

L'arborescence peut être organisée pour l'ensemble des responsables de la sécurité, à l'exception des responsables principaux de la sécurité. Les MSO sont affichés dans une liste à un niveau, sous le nœud du MSO. Le nœud des responsables de la sécurité comporte une arborescence dans laquelle chaque nœud représente un responsable de la sécurité. Toutefois, cette hiérarchie ne tient pas compte des droits et des rôles.

Condition préalable : pour déplacer un responsable de la sécurité dans l'arborescence, vous devez posséder le droit d'affichage et de modification de responsables de la sécurité.

Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, faites glisser le responsable que vous souhaitez déplacer vers le nœud approprié.

Tous les enfants du responsable sélectionné seront également déplacés.

7.15 Basculement rapide de responsables de la sécurité

À titre pratique, vous pouvez redémarrer rapidement SafeGuard Management Center afin de vous connecter sous le nom d'un autre responsable.

Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Fichier** > **Changer de responsable**. SafeGuard Management Center redémarre et la boîte de dialogue Connexion s'affiche.
2. Sélectionnez le responsable de la sécurité que vous souhaitez connecter à SafeGuard Management Center, puis entrez son mot de passe. Si vous travaillez en mode Multi Tenancy, vous serez connecté selon la même configuration de base de données.

SafeGuard Management Center redémarre et la vue attribuée au responsable connecté s'affiche.

7.16 Suppression d'un responsable de la sécurité

Condition préalable : pour supprimer un responsable de la sécurité ou un responsable principal de la sécurité, vous devez posséder le droit d'affichage et de suppression de responsables de la sécurité.

Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le responsable de la sécurité ou le responsable principal de la sécurité à supprimer et sélectionnez **Supprimer**. Vous ne pouvez pas supprimer le responsable de la sécurité sous le nom duquel vous êtes connecté.
3. Si le responsable possède des enfants, vous êtes invité à sélectionner un nouveau nœud parent pour les enfants.

Le responsable est supprimé de la base de données.

Avis : un responsable principal de la sécurité explicitement créé en tant que responsable et non seulement promu au rang de responsable de la sécurité doit cependant être conservé dans la base de données. Si un utilisateur promu au rang de responsable de la sécurité est supprimé de la base de données, son compte utilisateur l'est également.

Avis : si le responsable à supprimer s'est vu attribuer un rôle incluant une authentification supplémentaire et que le responsable est le seul à qui ce rôle a été attribué, le responsable sera tout de même supprimé. Nous considérons que le responsable principal de la sécurité sera en mesure de prendre le contrôle de l'autorisation supplémentaire.

8 Chiffrement de données

La fonction principale de SafeGuard Enterprise est le chiffrement des données sur des périphériques de stockage de données différents. Le chiffrement peut être basé sur volume ou sur fichier avec des clés et des algorithmes différents.

Les fichiers sont chiffrés de manière transparente. Lorsqu'un utilisateur ouvre, modifie et enregistre un fichier, il n'est pas invité à le chiffrer ou déchiffrer.

En tant que responsable de la sécurité, vous définissez les paramètres de chiffrement dans une stratégie de sécurité du type **Protection du périphérique**.

8.1 Chiffrement basé sur volume

Grâce au chiffrement basé sur volume, toutes les données d'un volume (y compris les fichiers d'initialisation, les fichiers paginés, les fichiers d'hibernation, les fichiers temporaires, les informations de répertoire, etc.) sont chiffrées. L'utilisateur n'a pas à modifier ses habitudes de travail ni tenir compte de problèmes de sécurité.

Avis : Si une stratégie de chiffrement existe pour un volume ou un type de volume et que le chiffrement du volume échoue, l'utilisateur n'est pas autorisé à y accéder.

Pour appliquer le chiffrement basé sur volume à des ordinateurs de points de terminaison, créez une stratégie du type **Protection du périphérique** et définissez le **Mode de chiffrement du support** sur **Sur volume**.

8.1.1 Chiffrement initial rapide

SafeGuard Enterprise propose une fonction de chiffrement initial rapide en tant que mode spécial du chiffrement basé sur volume. Il permet de réduire la durée nécessaire au chiffrement initial (ou final) de volumes sur des ordinateurs de points de terminaison en accédant uniquement à l'espace disque en cours d'utilisation.

Les conditions préalables suivantes s'appliquent au chiffrement initial rapide :

- Le chiffrement initial rapide s'applique aux volumes au format NTFS uniquement.
- Les volumes au format NTFS dont la taille de cluster est de 64 Ko ne peuvent pas être chiffrés en mode de chiffrement initial rapide.

Avis : Ce mode se traduit par une sécurité inférieure si un disque a déjà été utilisé précédemment avec SafeGuard Enterprise. Les secteurs inutilisés peuvent contenir des données. Le chiffrement initial rapide est donc désactivé par défaut.

Pour activer le chiffrement initial rapide, sélectionnez le paramètre **Chiffrement initial rapide** dans une stratégie du type **Protection du périphérique**.

Avis : Pour le déchiffrement d'un volume, le mode de chiffrement initial rapide est toujours utilisé quel que soit le paramètre de stratégie défini. Les conditions préalables indiquées s'appliquent également au déchiffrement.

8.1.2 Chiffrement basé sur volume et partition système Windows 7

Pour Windows 7 Professionnel, Entreprise et Édition Intégrale, une partition système est créée sur les ordinateurs de points de terminaison sans assignation de lettre de lecteur. Cette partition système ne peut pas être chiffrée par SafeGuard Enterprise.

8.1.3 Chiffrement basé sur volume et objets du système de fichiers non identifiés

Les objets du système de fichiers non identifiés sont des volumes qui ne peuvent pas être clairement identifiés comme texte brut ou chiffrés par SafeGuard Enterprise. L'accès au volume est refusé s'il existe une stratégie de chiffrement définie pour un objet du système de fichiers non identifiés. Si aucune stratégie de chiffrement n'existe, l'utilisateur peut accéder au volume.

Avis : Si une stratégie de chiffrement, dont le paramètre **Clé à utiliser pour le chiffrement** est défini de sorte à permettre la sélection de clé (par exemple, **Toute clé du jeu de clés utilisateur**) existe pour un volume d'objets du système de fichier non identifiés, un intervalle de temps s'écoule entre l'affichage de la boîte de dialogue de sélection de la clé et le refus de l'accès. Pendant cet intervalle, le volume reste accessible. Le volume est accessible tant que la boîte de dialogue de sélection de clé n'est pas confirmée. Pour éviter ceci, indiquez une clé présélectionnée pour le chiffrement. Cet intervalle de temps existe également pour les volumes d'objets du système de fichiers non identifiés qui sont connectés à un ordinateur de point de terminaison, notamment lorsque l'utilisateur a déjà ouvert des fichiers sur le volume lorsque la stratégie de chiffrement prend effet. Dans ce cas, il n'est pas garanti que l'accès au volume sera refusé car cela risque de provoquer une perte de données.

8.1.4 Chiffrement de volumes avec fonctionnalité d'exécution automatique activée

Si vous appliquez une stratégie de chiffrement aux volumes pour lesquels l'exécution automatique est activée, les problèmes suivants peuvent se produire :

- Le volume n'est pas chiffré.
- Si le volume est un objet du système de fichiers non identifié (see *Chiffrement basé sur volume et objets du système de fichiers non identifiés*, page 60), l'accès n'est pas refusé.

8.1.5 Accès aux volumes chiffrés BitLocker To Go

Si SafeGuard Enterprise est utilisé avec la prise en charge de BitLocker To Go activée et qu'une stratégie de chiffrement SafeGuard Enterprise existe pour un volume chiffré BitLocker To Go, l'accès au volume sera refusé. Si aucune stratégie de chiffrement SafeGuard Enterprise n'existe, l'utilisateur peut accéder au volume.

Avis : Si les paramètres d'exécution automatique d'une carte mémoire USB chiffrée BitLocker To Go sont définis sur les valeurs par défaut, il est possible que l'accès ne soit pas refusé même si une stratégie de chiffrement SafeGuard Enterprise existe. Ceci s'applique à Windows Vista uniquement.

8.2 Chiffrement basé sur fichier

Le chiffrement basé sur fichier garantit que toutes les données sont chiffrées (à l'exception du support d'initialisation et des informations de répertoire). Grâce au chiffrement basé sur fichier, même les supports optiques tels que les CD/DVD peuvent être chiffrés. De plus, les données peuvent être échangées avec des ordinateurs externes sur lesquels SafeGuard n'est pas installé (si les stratégies l'autorisent).

Avis : Les données chiffrées selon la méthode de chiffrement basé sur fichier ne peuvent pas être compressées. De même, les données compressées ne peuvent pas être chiffrées selon la méthode basée sur fichier.

Avis : Les volumes d'initialisation ne sont jamais chiffrés selon la méthode basée sur fichier. Ils seront automatiquement exclus du chiffrement basé sur fichier, même si une règle correspondante est définie.

Pour appliquer le chiffrement basé sur fichier à des ordinateurs de points de terminaison, créez une stratégie du type **Protection du périphérique** et définissez le **Mode de chiffrement** du support sur **Sur fichier**.

8.2.1 Exclusion d'applications du chiffrement

Vous pouvez définir des applications devant être ignorées par le pilote du filtre SafeGuard Enterprise et devant être exclues du chiffrement/déchiffrement transparent.

Un exemple est un programme de sauvegarde. Pour garantir que ces données ne sont pas déchiffrées lors de la création d'une sauvegarde, cette application peut être exclue du processus de chiffrement/déchiffrement. Les données sont sauvegardées sous forme chiffrée.

Un exemple type consiste à définir des programmes de sauvegarde comme exemptés afin qu'ils puissent toujours lire et enregistrer les données chiffrées.

Les applications susceptibles de déclencher des dysfonctionnements lorsqu'elles sont utilisées avec SafeGuard Enterprise mais qui ne nécessitent pas de chiffrement peuvent généralement être exemptées de chiffrement.

Vous pouvez définir des applications devant être exclues du chiffrement /déchiffrement dans une stratégie du type **Protection du périphérique** avec la cible **Périphériques de stockage locaux**. Le nom complet du fichier exécutable (contenant éventuellement les informations du chemin d'accès) est utilisé pour spécifier les **Applications non gérées**.

9 Gestion des clés de SafeGuard Enterprise

Lors de l'importation de la structure du répertoire, la version standard de SafeGuard Enterprise génère automatiquement des clés pour :

- Domaines
- Conteneurs/OU
- Groupes

et les attribue aux objets correspondants. Des clés d'ordinateur et d'utilisateur sont générées selon les besoins.

Les clés ne peuvent pas être supprimées. Elles sont conservées en permanence dans la base de données de SafeGuard Enterprise.

Lorsqu'un ordinateur final est initialisé pour la première fois, SafeGuard Enterprise génère une clé d'ordinateur pour cet ordinateur (clé machine définie).

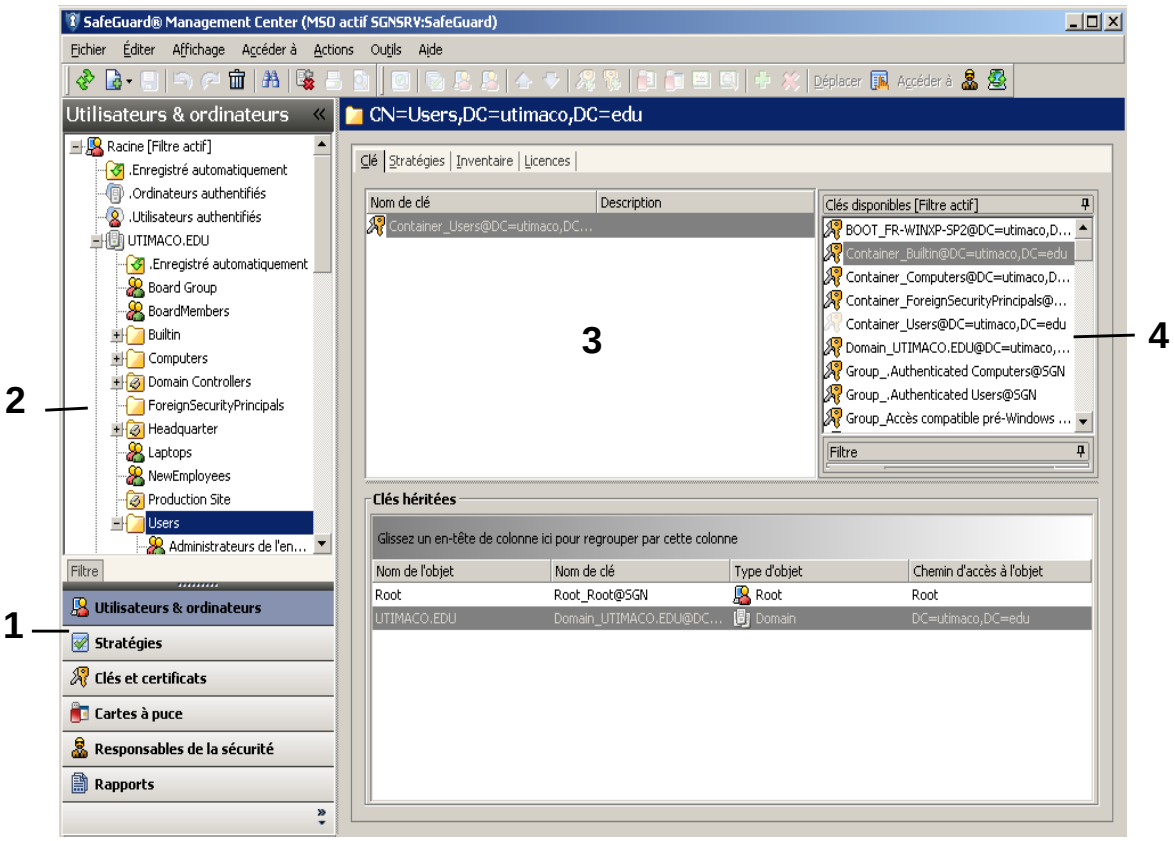
Chaque utilisateur obtient toutes ses clés lors de la connexion à partir de son jeu de clés. Le jeu de clés d'un utilisateur comporte les éléments suivants :

- une clé personnelle ;
- les clés des groupes auxquels appartient l'utilisateur ;
- les clés des conteneurs/OU globaux des groupes auxquels appartient l'utilisateur.

Les clés du jeu de clés de l'utilisateur déterminent les données auxquelles l'utilisateur peut accéder. L'utilisateur ne peut accéder qu'aux données pour lesquelles il possède une clé spécifique.

Pour afficher toutes les clés d'un utilisateur, cliquez sur **Utilisateurs & ordinateurs**, puis sélectionnez l'onglet **Clés**.

Pour afficher toutes les clés, cliquez sur **Clés et certificats** dans SafeGuard Management Center. Vous pouvez générer des listes de **Clés attribuées** et de **Clés inactives**.

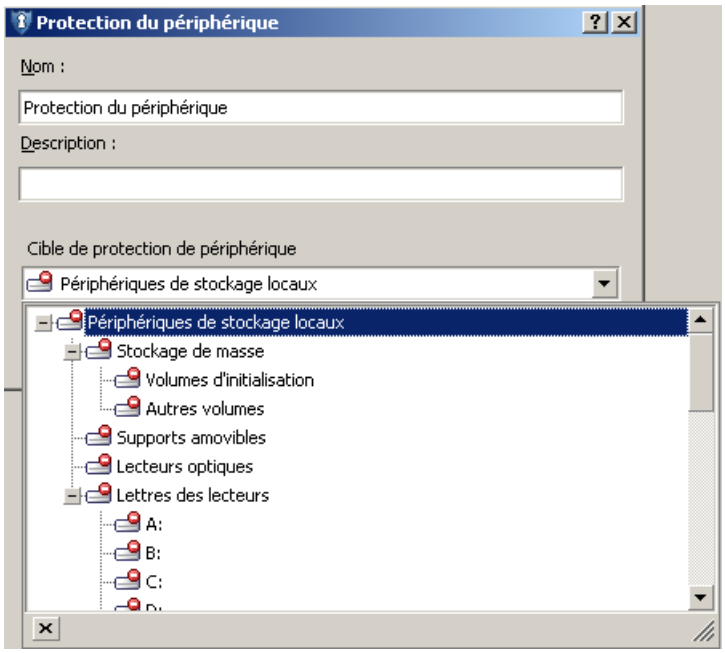


1. Cliquez sur **Utilisateurs & ordinateurs** pour ouvrir l'écran.
2. Les clés de tous les objets cochés sont affichées dans la zone action et dans les vues respectives.
3. Zone Action : l'écran dépend des sélections dans la zone de navigation. Toutes les clés attribuées à l'objet sont affichées.
4. Toutes les clés disponibles sont affichées ici. Les clés déjà attribuées à l'objet sélectionné sont grisées. Sélectionnez **Filtre** pour basculer entre des clés déjà attribuées à un objet (actives) et des clés non attribuées à un objet (inactives).

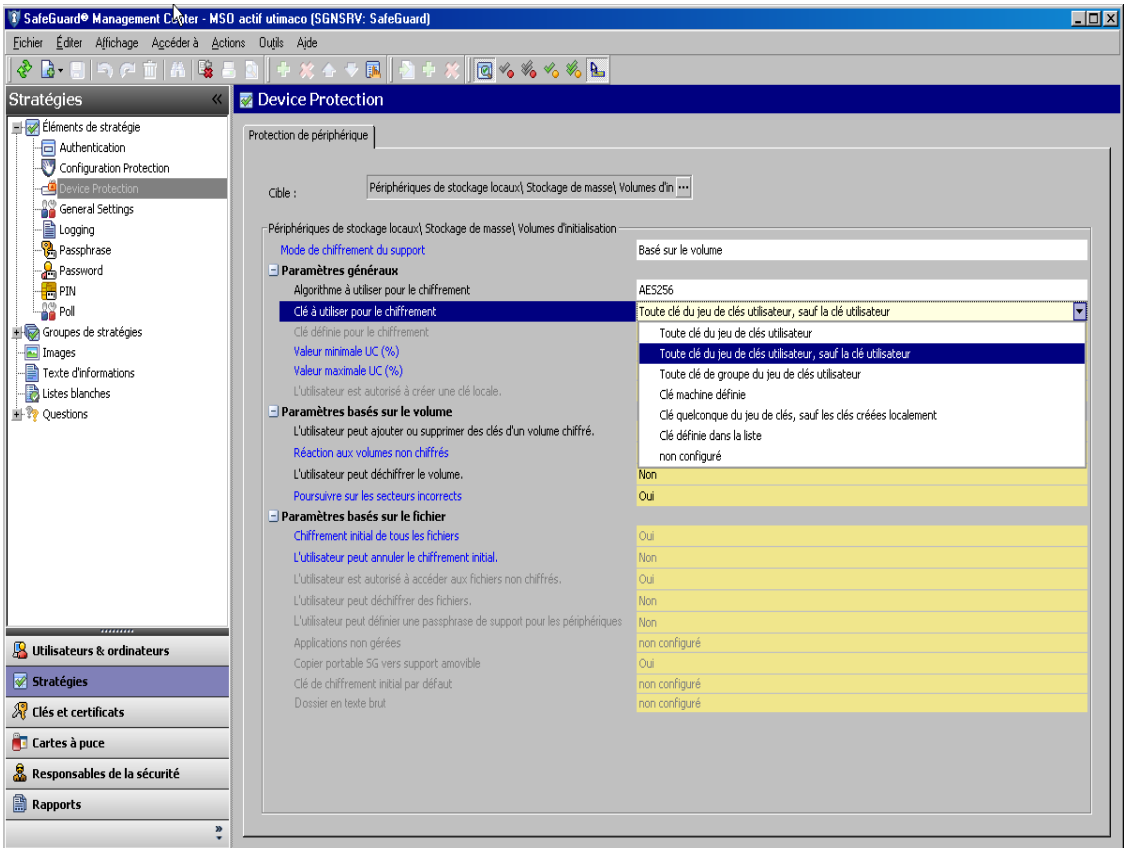
Après l'importation, chaque utilisateur reçoit un certain nombre de clés utilisables pour le chiffrement des données.

9.1 Clés pour le chiffrement des données

Des clés sont attribuées aux utilisateurs pour le chiffrement de volumes spécifiques lors de la définition de stratégies du type Protection du périphérique. Les volumes sont les suivants :



Lorsque vous définissez les paramètres pour chaque support, l'option suivante est proposée : **Clé à utiliser pour le chiffrement**.


SafeGuard® Management Center - MSO actif utimaco (SGNSRV: SafeGuard)
Fichier Éditer Affichage Accéder à Actions Outils Aide
Stratégies
Éléments de stratégie
Authentication
Configuration Protection
Device Protection
General Settings
Logging
Passphrase
Password
PIN
Poll
Groupes de stratégies
Images
Texte d'informations
Listes blanches
Questions
Utilisateurs & ordinateurs
Stratégies
Clés et certificats
Cartes à puce
Responsables de la sécurité
Rapports
Device Protection
Protection de périphérique
Cible :
Périphériques de stockage locaux\ Stockage de masse\ Volumes d'in
Périphériques de stockage locaux\ Stockage de masse\ Volumes d'initialisation
Mode de chiffrement du support
Basé sur le volume
Paramètres généraux
Algorithme à utiliser pour le chiffrement
AES256
Clé à utiliser pour le chiffrement
Toute clé du jeu de clés utilisateur, sauf la clé utilisateur
Clé définie pour le chiffrement
Valeur minimale UC (%)
Valeur maximale UC (%)
L'utilisateur est autorisé à créer une clé locale.
Paramètres basés sur le volume
L'utilisateur peut ajouter ou supprimer des clés d'un volume chiffré.
Réaction aux volumes non chiffrés
L'utilisateur peut déchiffrer le volume.
Non
Poursuivre sur les secteurs incorrects
Oui
Paramètres basés sur le fichier
Chiffrement initial de tous les fichiers
Oui
L'utilisateur peut annuler le chiffrement initial.
Non
L'utilisateur est autorisé à accéder aux fichiers non chiffrés.
Oui
L'utilisateur peut déchiffrer des fichiers.
Non
L'utilisateur peut définir une passphrase de support pour les périphériques
Non
Applications non gérées
non configuré
Copier portable SG vers support amovible
Oui
Clé de chiffrement initial par défaut
non configuré
Dossier en texte brut
non configuré
Toute clé du jeu de clés utilisateur
Toute clé du jeu de clés utilisateur, sauf la clé utilisateur
Toute clé de groupe du jeu de clés utilisateur
Clé machine définie
Clé quelconque du jeu de clés, sauf les clés créées localement
Clé définie dans la liste
non configuré

Ici, vous pouvez décider quelles sont les clés que l'utilisateur peut ou doit utiliser pour le chiffrement :

- **Toute clé du jeu de clés utilisateur**
  Après s'être connectés, les utilisateurs Windows peuvent sélectionner les clés qu'ils souhaiteraient utiliser pour chiffrer un volume particulier.
  Une boîte de dialogue s'affiche pour permettre à l'utilisateur de sélectionner la clé de son choix.

- **Toute clé du jeu de clés utilisateur sauf la clé utilisateur**
  Un utilisateur n'est pas autorisé à utiliser sa clé personnelle pour chiffrer des données.

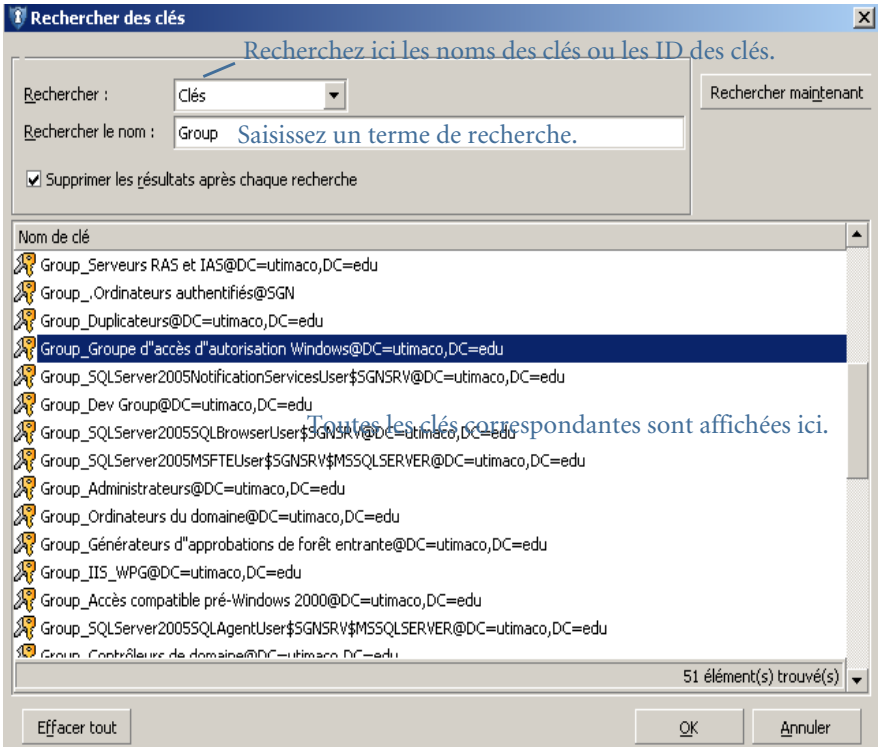
- **Toute clé de groupe du jeu de clés utilisateur**
  L'utilisateur ne peut sélectionner qu'une des clés de groupe présentes dans son jeu de clés.

- **Clé ordinateur définie**
  C'est la clé unique générée exclusivement pour cet ordinateur par SafeGuard Enterprise lorsque cette machine est initialisée pour la première fois. L'utilisateur n'a pas d'autre option. Une clé définie par l'ordinateur est généralement utilisée par la partition d'initialisation et système et pour les unités sur lesquelles se trouve le répertoire Documents and Settings.

- **Clé définie dans la liste**
  Cette option permet de définir une clé particulière que l'utilisateur doit utiliser pour le chiffrement. Pour spécifier une clé d'un utilisateur de cette manière, vous devez définir une clé sous **Clé définie pour le chiffrement** (s'affiche lorsque vous sélectionnez **Clé définie dans la liste**).

  Cliquez sur le bouton [**...**] situé en regard de l'option **Clé définie pour le chiffrement** pour afficher une boîte de dialogue dans laquelle vous pouvez spécifier une clé.

  Assurez-vous que l'utilisateur est également en possession de la clé correspondante pour spécifier des clés de cette manière.



Mettez en surbrillance la clé sélectionnée et cliquez sur **OK**.
La clé sélectionnée sera utilisée pour le chiffrement sur l'ordinateur final.

9.2 Certificats

- SafeGuard Enterprise peut être vérifié par des certificats signés SHA1, MD2 et MD55.
- Si des certificats de l'autorité de certification (AC) sont supprimés dans la base de données et si vous ne souhaitez plus les utiliser, vous devez les supprimer manuellement de tous les PC d'administration du magasin local.
- SafeGuard Enterprise ne peut ensuite communiquer avec les certificats ayant expiré que si les clés nouvelles et anciennes sont présentes sur la même carte.
- La combinaison de certificats de l'AC et de CRL (liste de révocation des certificats) d'une carte à puce doit correspondre. Dans le cas contraire, les utilisateurs ne peuvent pas se connecter à leurs ordinateurs respectifs. Vérifiez que la combinaison est correcte. SafeGuard Enterprise n'effectue pas cette vérification.
- Les certificats de connexion des responsables de la sécurité doivent se trouver dans « MY ».
- Les certificats de l'AC ne peuvent pas provenir d'une clé cryptographique et être stockés dans la base de données ou dans le magasin de certificats. Si vous souhaitez (ou si vous avez besoin) d'utiliser des certificats de l'AC, ces derniers doivent être disponibles sous forme de fichier et pas seulement sous forme de clé cryptographique. Ceci s'applique également aux CRL.
- Notez que lors de l'importation d'un certificat utilisateur, la section publique et la section privée de ce certificat sont importées toutes les deux. Si uniquement la partie publique est importée, seule l'authentification par clé cryptographique est prise en charge.

9.3 Clients virtuels

Les clients virtuels sont des fichiers de clés spécifiques pouvant être utilisés pour la récupération dans une procédure Challenge/Réponse lorsque les informations utilisateur requises ne sont pas disponibles et lorsque la procédure Challenge/Réponse n'est généralement pas prise en charge, lorsque POA est corrompu par exemple.

Pour activer une procédure challenge/réponse dans cette situation d'urgence complexe, vous pouvez créer des fichiers spécifiques, appelés clients virtuels, et vous devez les distribuer à l'utilisateur avant la session de challenge/réponse. La procédure de challenge/réponse peut ensuite être initiée à l'aide de ces clients virtuels via un outil de récupération de clé sur l'ordinateur final. Il suffit ensuite à l'utilisateur d'informer le responsable support de la ou des clés requises et de saisir le code de réponse afin de pouvoir accéder à nouveau aux volumes chiffrés.

La récupération est possible à l'aide d'une seule clé ou en utilisant un fichier de clés chiffré en contenant plusieurs.

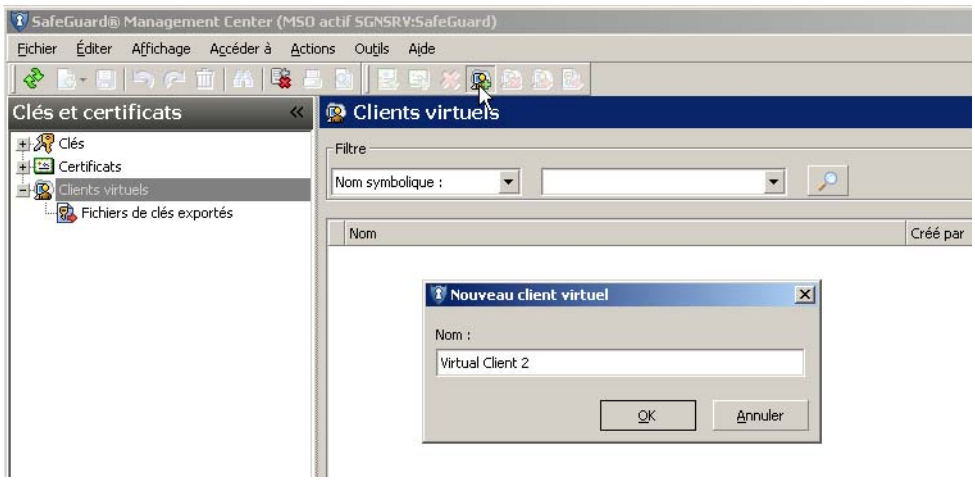
La zone **Clés et certificats** de SafeGuard Management Center vous permet d'effectuer les tâches suivantes :

- créer et exporter des clients virtuels ;
- créer et exporter des fichiers de clés chiffrés contenant plusieurs clés ;
- afficher et filtrer des clients virtuels et des fichiers de clés exportés ;
- supprimer des clients virtuels.

9.3.1 Création de clients virtuels

Les fichiers du client virtuel peuvent être utilisés par différents ordinateurs et pour plusieurs sessions de challenge/réponse.

1. Ouvrez SafeGuard Management Center et cliquez sur **Clés et certificats**.
2. Cliquez sur **Clients virtuels** dans la fenêtre de navigation de gauche.



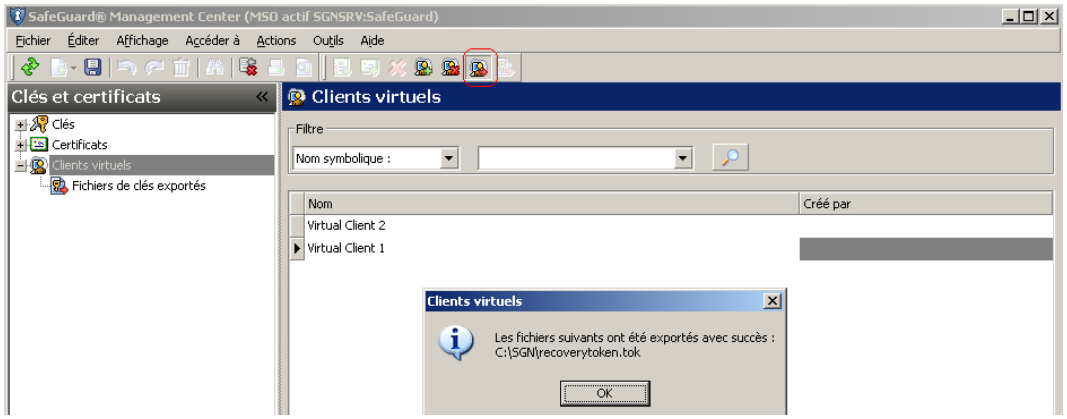
3. Dans la barre d'outils, cliquez sur **Ajouter un client virtuel**.
4. Entrez un nom unique pour le client virtuel et cliquez sur **OK**. Les clients virtuels sont identifiés dans la base de données par ces noms.
5. Enregistrez le client virtuel dans la base de données en cliquant sur l'icône **Enregistrer** de la barre d'outils.

Le nouveau client virtuel s'affiche dans la zone d'action.

9.3.2 Exportation de clients virtuels

Une fois le client virtuel créé, vous devez l'exporter dans un fichier. Ce fichier est toujours nommé `recoverytoken.tok` et doit être distribué au support. Ce fichier doit être disponible dans l'environnement de l'ordinateur final au démarrage d'une session de challenge/réponse via un outil de récupération, lorsque POA est corrompu par exemple. L'utilisateur doit placer le fichier de client virtuel, `recoverytoken.tok`, dans le même dossier que l'outil de récupération pour la prise en charge d'une session de challenge/réponse.

1. Ouvrez SafeGuard Management Center et cliquez sur **Clés et certificats**.
2. Cliquez sur **Clients virtuels** dans la fenêtre de navigation de gauche.



3. Dans la zone d'action, recherchez le client virtuel concerné en cliquant sur la loupe. Les clients virtuels disponibles s'affichent.
4. Sélectionnez l'entrée requise dans la zone d'action et cliquez sur **Exporter le client virtuel** dans la barre d'outils.
5. Sélectionnez l'emplacement de stockage du fichier `recoverytoken.tok` et cliquez sur **OK**.
6. Un message indiquant le stockage réussi et l'emplacement du fichier s'affiche.
7. Distribuez ce fichier de client virtuel, `recoverytoken.tok`, aux utilisateurs de SafeGuard Enterprise concernés.

Conservez ce fichier en lieu sûr, sur une carte mémoire par exemple. Dans le cadre d'une session de challenge/réponse, ce fichier doit se trouver dans le même dossier que l'outil de récupération.

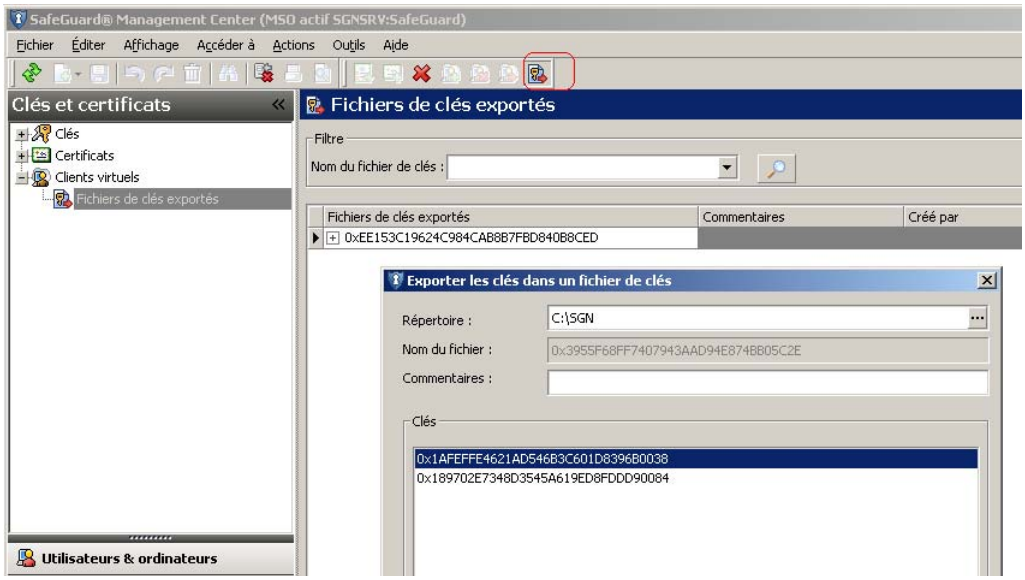
9.3.3 Création et exportation de fichiers de clés pour la récupération des clients virtuels

Lorsque plusieurs clés sont requises pour pouvoir de nouveau accéder à des volumes chiffrés lors de la récupération d'un client virtuel, le responsable de la sécurité peut les combiner dans un fichier exporté. Ce fichier de clés est chiffré à l'aide d'un mot de passe aléatoire, qui est stocké dans la base de données. Ce mot de passe est propre à chaque fichier de clés créé.

Le fichier de clés chiffré doit être transmis à l'utilisateur et l'utilisateur doit l'avoir au démarrage d'une session de challenge/réponse via un outil de récupération.

Dans la session de challenge/réponse, le mot de passe du fichier de clés est transmis avec le code de réponse. Le fichier de clés peut alors être déchiffré avec le mot de passe et tous les volumes chiffrés avec les clés disponibles sont de nouveau accessibles.

1. Ouvrez SafeGuard Management Center et cliquez sur **Clés et certificats**.
2. Cliquez sur **Clients virtuels** puis sur **Fichiers de clés exportés** dans la fenêtre de navigation de gauche.



3. Dans la barre d'outils, cliquez sur **Nouveau fichier de clés d'exportation**.
4. Dans **Exporter les clés dans un fichier de clés**, entrez les informations suivantes :
   - **Répertoire :** Cliquez sur **[...]** pour sélectionner l'emplacement du fichier de clés.
   - **Nom du fichier :** Le fichier de clés est chiffré à l'aide d'un mot de passe aléatoire qui s'affiche dans **Nom du fichier**. Vous ne pouvez pas modifier ce nom.

- Cliquez sur **Ajouter une clé** ou sur **Supprimer une clé** pour ajouter ou supprimer des clés. Une fenêtre contextuelle s'affiche pour rechercher et sélectionner les clés requises. Confirmez la sélection en cliquant sur **OK**.
- Cliquez sur **OK** pour confirmer toutes les saisies.

5. Distribuez le fichier de clés dans l'environnement des ordinateurs finaux concernés. Ils doivent l'avoir avant de saisir le code de réponse sur le client.

9.3.4 Affichage et filtrage des vues Client virtuel

Pour rechercher plus facilement le client virtuel ou des clés requis pendant une session de challenge/réponse, il existe plusieurs possibilités de filtrage et de recherche dans SafeGuard Management Center, sous Clés et certificats.

Vues des clients virtuels

1. Cliquez sur **Clients virtuels** dans la fenêtre de navigation de gauche.
2. Cliquez sur la loupe pour générer la liste complète de tous les clients virtuels.
3. Filtrez les clients virtuels par **Nom symbolique** ou par **GUID de clé**.

Vues des fichiers de clés exportés

1. Cliquez sur **Clients virtuels**, puis sur **Fichiers de clés exportés**.
2. Cliquez sur la loupe pour générer la liste complète de tous les fichiers de clés exportés.
3. Cliquez sur l'icône + située en regard du fichier de clés requis pour afficher les clés contenues dans ce fichier.

9.3.5 Suppression de clients virtuels

Pour supprimer un client virtuel, procédez de la façon suivante :

1. Ouvrez SafeGuard Management Center et cliquez sur **Clés et certificats**.
2. Cliquez sur **Clients virtuels** dans la fenêtre de navigation de gauche.
3. Dans la zone d'action, recherchez le client virtuel concerné en cliquant sur la loupe. Les clients virtuels disponibles s'affichent.
4. Sélectionnez l'entrée requise dans la zone d'action et cliquez sur **Supprimer le client virtuel** dans la barre d'outils.

5. Enregistrez les modifications dans la base de données en cliquant sur l'icône Enregistrer de la barre d'outils.

Le client virtuel est supprimé de la base de données.

10 Utilisation de stratégies

Les sections suivantes décrivent les tâches administratives relatives aux stratégies, par exemple la création, le regroupement et la sauvegarde.

Tous les paramètres de stratégie disponibles dans SafeGuard Enterprise sont décrits dans la section Stratégies de sécurité.

10.1 Création de stratégies

Pour créer une stratégie, procédez comme suit :

1. Connectez-vous à SafeGuard Management Center à l'aide du mot de passe défini lors de la configuration initiale.
2. Cliquez sur **Stratégies** dans la zone de navigation.
3. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Éléments de stratégie**, puis sélectionnez **Nouveau**.
4. Sélectionnez le type de stratégie. Une boîte de dialogue pour nommer la stratégie du type de stratégie sélectionné s'affiche.
5. Entrez le nom et éventuellement la description de la nouvelle stratégie.

   Stratégies de protection du périphérique :

   Lors de la création d'une stratégie de protection du périphérique, vous devez également spécifier la cible de la protection du périphérique dans cette boîte de dialogue. Les cibles possibles sont les suivantes :

- stockage de masse (volumes d'initialisation/autres volumes) ;
- supports amovibles ;
- lecteurs optiques ;

  Une stratégie distincte doit être créée pour chaque cible. Vous pouvez ultérieurement combiner les stratégies individuelles dans un groupe de stratégies nommé *Chiffrement* par exemple.

6. Cliquez sur **OK**.

La nouvelle stratégie s'affiche dans la fenêtre de navigation sous **Éléments de stratégie**. Tous les paramètres du type de stratégie sélectionné s'affichent dans la zone d'action.

10.2 Édition de paramètres de stratégie

Lors de la sélection d'une stratégie dans la fenêtre de navigation, vous pouvez éditer les paramètres de la stratégie dans la zone d'action.

	Une icône rouge en regard d'un paramètre « non configuré » indique qu'une valeur doit être définie pour ce paramètre de stratégie. Pour enregistrer la stratégie, vous devez tout d'abord sélectionner un paramètre autre que non configuré.

10.2.1 Restauration des valeurs par défaut de paramètres de stratégie

Dans la barre d'outils, les icônes suivantes servent à la configuration des paramètres de stratégie :

	Affiche les valeurs par défaut des paramètres de stratégie non configurés.
	Définit le paramètre de stratégie marqué comme « non configuré ».
	Définit tous les paramètres de stratégie d'une zone sur « non configuré ».
	Définit la valeur par défaut de la stratégie marquée.
	Définit tous les paramètres de stratégie d'une zone sur la valeur par défaut.

10.2.2 Différences entre les stratégies spécifiques d'une machine et les stratégies spécifiques d'un utilisateur

Stratégie de couleur bleue	La stratégie s'applique uniquement aux machines et non aux utilisateurs.
Stratégie de couleur noire	La stratégie s'applique aux machines et aux utilisateurs.

10.3 Groupes de stratégies

Les stratégies SafeGuard Enterprise doivent être combinées dans des groupes de stratégies. Un groupe de stratégies peut contenir différents types de stratégies.

Si vous rassemblez des stratégies du même type dans un groupe, les paramètres sont fusionnés automatiquement. Dans ce cas, vous pouvez définir des priorités d'utilisation des paramètres. Les paramètres d'une stratégie ayant une priorité supérieure remplacent ceux d'une stratégie de priorité inférieure. Si une option est définie sur **non configuré**, le paramètre **ne sera pas remplacé** dans une stratégie de priorité inférieure.

Exception relative à la protection du périphérique :

Les stratégies de protection du périphérique seront fusionnées uniquement si certaines sont définies pour la même cible (volume d'initialisation par exemple). Les paramètres sont ajoutés si elles pointent des cibles différentes.

10.3.1 Combinaison de stratégies dans des groupes

Les stratégies individuelles de différents types doivent être tout d'abord créées.

Pour les stratégies dans des groupes, procédez comme suit :

1. Cliquez sur **Stratégies** dans la zone de navigation.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Groupes de stratégies** et sélectionnez **Nouveau**.
3. Cliquez sur **Nouveau groupe de stratégies**. Une boîte de dialogue pour nommer le groupe de stratégies s'affiche.
4. Entrez le nom et éventuellement la description du groupe de stratégies. Cliquez ensuite sur **OK**.
5. Le nouveau groupe de stratégies s'affiche dans la **fenêtre de navigation** sous **Groupes de stratégies**.
6. Sélectionnez le groupe de stratégies. La zone d'action indique tous les éléments requis pour regrouper les stratégies.
7. Pour ajouter les stratégies au groupe, glissez-les de la liste de stratégies disponibles dans la zone de stratégies.
8. Vous pouvez définir une **priorité** pour chaque stratégie en les organisant grâce au menu contextuel.

Si vous rassemblez des stratégies du même type dans un groupe, les paramètres sont fusionnés automatiquement. Dans ce cas, vous pouvez définir des priorités d'utilisation des paramètres. Les paramètres d'une stratégie ayant une priorité supérieure remplacent ceux d'une stratégie de priorité inférieure. Si une option est définie sur **non configuré**, le paramètre **ne sera pas remplacé** dans une stratégie de priorité inférieure.

Exception relative à la protection du périphérique :

Les stratégies de protection du périphérique seront fusionnées uniquement si certaines sont définies pour la même cible (volume d'initialisation par exemple). Les paramètres sont ajoutés si elles pointent des cibles différentes.

9. Enregistrez la stratégie via **Fichier > Enregistrer**.

Le groupe de stratégies contient désormais les paramètres de toutes les stratégies individuelles.

10.3.2 Résultats du regroupement de stratégies

Le résultat du regroupement de stratégies s'affiche séparément.

Pour afficher le résultat, cliquez sur l'onglet **Résultat**.

- Un onglet distinct s'affiche pour chaque type de stratégie.

  Les paramètres obtenus de la combinaison des stratégies individuelles dans un groupe s'affichent.

- Pour les stratégies de protection du périphérique, un onglet s'affiche pour chaque cible de stratégie (volumes d'initialisation, lecteur X, etc.).

10.4 Sauvegarde de stratégies et de groupes de stratégies

Vous pouvez créer des sauvegardes de stratégies et de groupes de stratégies dans des fichiers XML. Si nécessaire, les stratégies/groupes de stratégies correspondants peuvent ensuite être restaurés à partir de ces fichiers XML.

Pour créer une sauvegarde d'une stratégie/d'un groupe de stratégies :

1. Sélectionnez la stratégie/le groupe de stratégies dans la fenêtre de navigation sous **Éléments de stratégie** ou **Groupes de stratégies**.

2. Cliquez avec le bouton droit de la souris pour afficher le menu contextuel et sélectionnez **Sauvegarder la stratégie**.

La commande **Sauvegarder la stratégie** est également accessible dans le menu **Actions**.

3. Dans la boîte de dialogue **Enregistrer sous**, entrez le nom du fichier XML, puis sélectionnez un emplacement de stockage. Cliquez sur **Enregistrer**.

La sauvegarde de la stratégie/du groupe de stratégies est stockée sous forme de fichier XML dans le répertoire spécifié.

10.5 Restauration de stratégies et de groupes de stratégies

Pour restaurer une stratégie/un groupe de stratégies à partir d'un fichier XML, procédez comme suit :

1. Sélectionnez les **Éléments de stratégie/Groupes de stratégies** dans la fenêtre de navigation.
2. Cliquez avec le bouton droit de la souris pour afficher le menu contextuel et sélectionnez **Restaurer une stratégie**.

   La commande **Restaurer une stratégie** est également accessible depuis le menu **Actions**.
3. Sélectionnez le fichier XML à partir duquel la stratégie/le groupe de stratégies doit être restauré, puis cliquez sur **Ouvrir**.

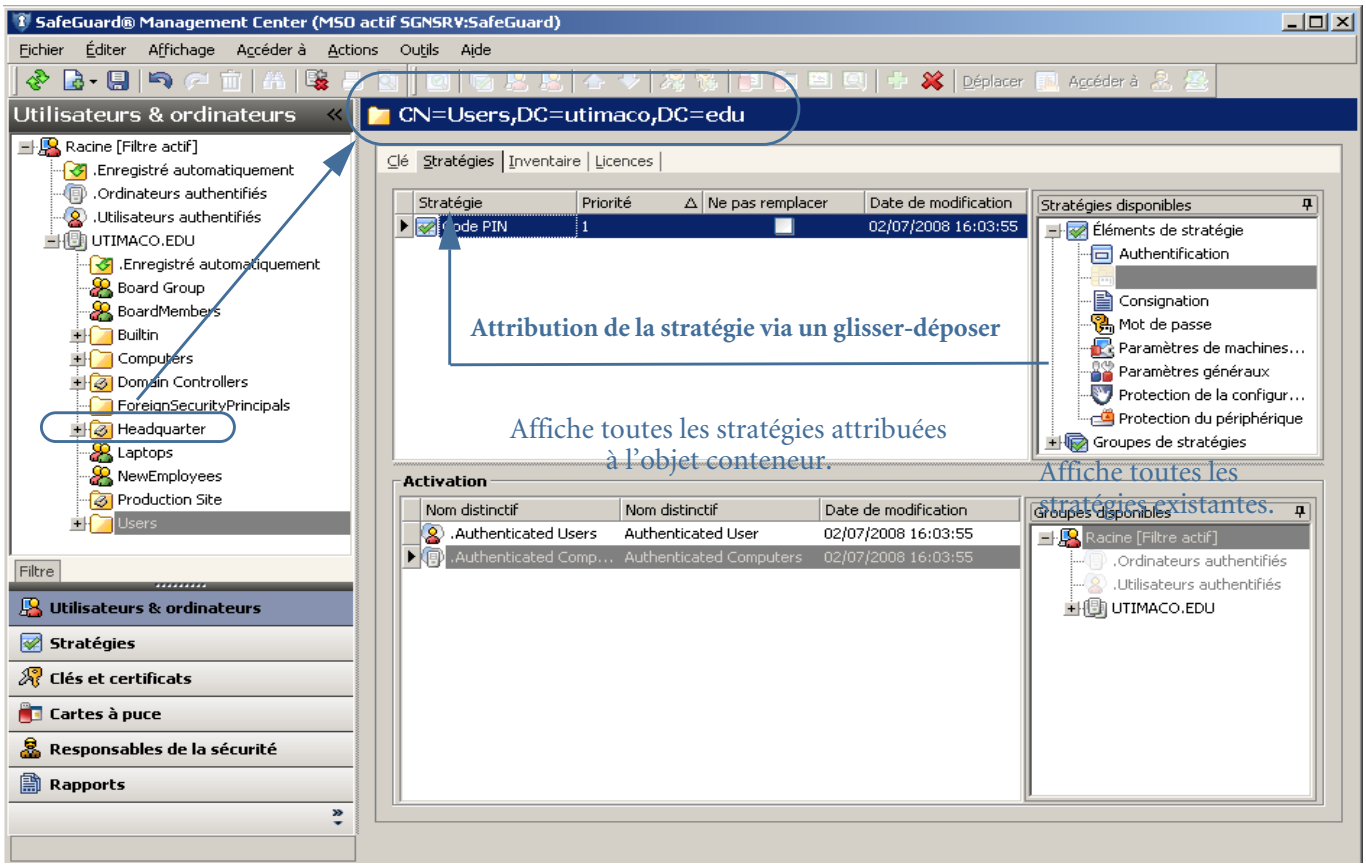
La stratégie/le groupe de stratégie est restauré(e).

10.6 Attribution des stratégies

Pour **attribuer** des stratégies, procédez de la façon suivante :

1. Cliquez sur **Utilisateurs & ordinateurs**. Sélectionnez l'objet conteneur (par exemple OU ou domaine) dans la fenêtre de navigation. Cliquez sur l'onglet **Stratégies** le cas échéant.

   Tous les éléments requis pour l'attribution de la stratégie sont affichés dans la zone d'action.

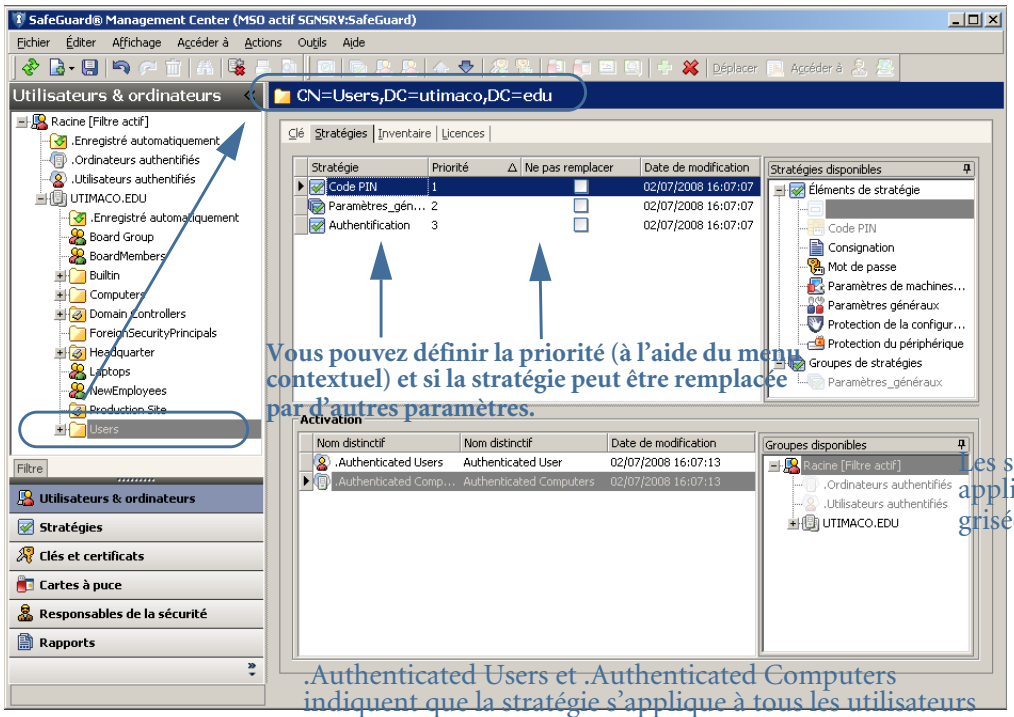


2. Pour attribuer une stratégie, faites-la glisser de la liste dans la zone de stratégie.

3. Vous pouvez définir une **Priorité** pour chaque stratégie en les organisant grâce au menu contextuel. Les paramètres des stratégies de niveau supérieur remplacent celles qui lui sont inférieures.

   Si vous sélectionnez **Ne pas remplacer** pour une stratégie, ses paramètres ne sont pas remplacés par ceux d'autres stratégies.

Avis : si vous sélectionnez **Ne pas remplacer** pour une stratégie de priorité inférieure, celle-ci acquiert une priorité plus élevée que celle d'une stratégie de niveau supérieur.



4. Les utilisateurs authentifiés et les ordinateurs authentifiés sont affichés dans la zone d'activation.

La stratégie s'applique à présent à tous les groupes au sein du OU et/ou du domaine.

10.6.1 Activation des stratégies pour des groupes individuels

Les stratégies sont toujours attribuées à un OU, à un domaine ou à un groupe de travail. Elles s'appliquent par défaut à tous les groupes de ces objets conteneurs (les utilisateurs authentifiés et les ordinateurs authentifiés sont affichés dans la zone d'activation).

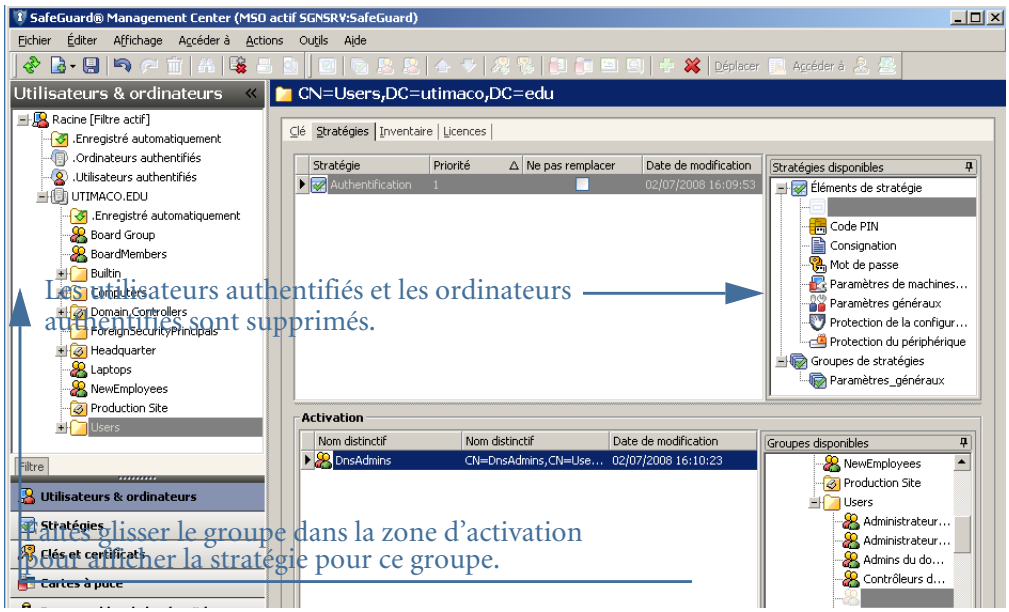
Toutefois, vous pouvez également définir des stratégies et les activer pour un ou plusieurs groupes. Ces stratégies s'appliquent ensuite exclusivement à ces groupes.

Pour définir une stratégie à n'appliquer qu'à un groupe spécifique, procédez de la façon suivante :

1. Attribuez la stratégie au OU contenant le groupe.
2. Les utilisateurs authentifiés et les ordinateurs authentifiés sont affichés dans la zone d'activation.

3. Faites glisser ces deux groupes de la zone d'activation jusqu'à la liste des groupes disponibles. Dans cette constellation, la stratégie n'est pas effective pour les utilisateurs ou les ordinateurs.

4. À présent, faites glisser le groupe requis (ou plusieurs groupes) de la liste des groupes disponibles jusqu'à la zone d'activation.


SafeGuard® Management Center (MSO actif SGNSRV:SafeGuard)
Les utilisateurs authentifiés et les ordinateurs authentifiés sont supprimés.
Faites glisser le groupe dans la zone d'activation pour afficher la stratégie pour ce groupe.

Cette stratégie s'applique désormais exclusivement à ce groupe.

Si des stratégies ont également été attribuées au OU de niveau supérieur, cette stratégie s'applique à ce groupe en plus de celles définies pour le OU entier.

10.7 Désactivation du déploiement de stratégies

Les responsables de la sécurité peuvent désactiver le déploiement des stratégies au niveau des ordinateurs finaux via le bouton **Activer/désactiver le déploiement des stratégies** dans la barre d'outils de SafeGuard Management Center ou en sélectionnant la commande **Activer/désactiver le déploiement des stratégies** dans le menu **Éditer**. Lorsque vous cliquez sur le bouton, sélectionnez la commande ou appuyez sur la touche F3, aucune stratégie n'est transmise aux ordinateurs finaux. En répétant le clic sur le bouton, la sélection de la commande ou l'appui sur la touche F3, vous pouvez réactiver le déploiement des stratégies et celles-ci sont de nouveau transmises.

Avis : pour désactiver le déploiement de stratégies, un responsable de la sécurité doit disposer du droit « Activer/désactiver le déploiement des stratégies ». Ce droit est attribué par défaut aux rôles Responsable principal de la sécurité et Responsable de la sécurité prédéfinis. Ce droit peut cependant être également attribué aux nouveaux rôles définis par l'utilisateur.

10.8 Règles d'attribution et d'analyse des stratégies

La gestion et l'analyse des stratégies s'effectuent selon les règles définies dans ce chapitre.

10.8.1 Attribution et activation des stratégies

Pour activer une stratégie devant être mise en œuvre pour un utilisateur ou un ordinateur, vous devez d'abord l'attribuer à un objet conteneur (nœuds racine, domaine, OU, conteneur intégré ou groupe de travail). Pour que la stratégie attribuée à un utilisateur ou à un ordinateur devienne effective, lorsque vous attribuez une stratégie à un point quelconque de la hiérarchie, tous les ordinateurs (ordinateurs authentifiés) et tous les utilisateurs (utilisateurs authentifiés) sont activés automatiquement (l'attribution sans activation ne suffit pas). Tous les utilisateurs et tous les ordinateurs sont combinés dans ces groupes.

10.8.2 Héritage de stratégie

Les stratégies ne peuvent être transmises qu'entre des objets conteneurs. Seuls des objets conteneurs peuvent transmettre des stratégies d'objets conteneurs d'un niveau supérieur. Les stratégies peuvent être activées au sein d'un conteneur à supposer qu'il ne contienne aucun autre objet conteneur (au niveau du groupe). L'héritage est impossible entre des groupes.

10.8.3 Hiérarchie d'héritage de stratégie

Lorsque des stratégies sont attribuées le long d'une chaîne hiérarchique, la stratégie mise en œuvre est celle ayant le niveau le plus élevé ; la plus proche dans le cas d'un objet cible (utilisateur/ordinateur). Cela signifie que si la distance entre une stratégie et l'objet cible s'accroît, elle sera remplacée par d'autres stratégies plus proches.

10.8.4 Attribution directe et indirecte des stratégies

Attribution directe

L'utilisateur/ordinateur reçoit une stratégie attribuée directement à l'objet conteneur dans lequel il se trouve (l'appartenance n'est pas suffisante). L'objet conteneur n'a pas transmis cette stratégie.

Attribution indirecte

L'utilisateur/ordinateur reçoit une stratégie que l'objet conteneur dans lequel il se trouve actuellement (l'appartenance en tant qu'utilisateur d'un groupe situé dans un autre objet conteneur n'est pas suffisante) a hérité d'un objet conteneur de niveau supérieur.

10.8.5 Activation/désactivation de stratégies

Pour qu'une stratégie soit effective pour un ordinateur/utilisateur, elle doit être activée au niveau du groupe (les stratégies ne peuvent être activées qu'au niveau du groupe). Que ce groupe se trouve ou non dans le même objet conteneur n'a pas d'importance. Le seul point important est que l'utilisateur ou l'ordinateur ait été attribué directement ou indirectement (par héritage) à la stratégie.

Si un ordinateur ou un utilisateur se trouve en dehors d'un OU, ou d'une ligne d'héritage, et fait partie d'un groupe qui se trouve lui-même dans ce OU, cette activation ne s'applique **pas** à cet utilisateur ou à cet ordinateur. En effet, il n'existe pas d'attribution valide pour cet utilisateur ou cet ordinateur (directement ou indirectement). Le groupe a bien été activé, mais l'activation ne peut s'appliquer qu'aux utilisateurs et aux machines pour lesquels il existe également une attribution de stratégie. En d'autres termes, l'activation des stratégies ne s'applique pas en dehors des limites des conteneurs s'il n'existe aucune attribution de stratégie directe ou indirecte pour cet objet.

Une stratégie devient effective lorsqu'elle a été activée pour des groupes d'utilisateurs ou des groupes d'ordinateurs. Les groupes d'utilisateurs puis les groupes d'ordinateurs sont analysés (les utilisateurs authentifiés et les ordinateurs authentifiés sont également des groupes). Les deux résultats sont reliés par une instruction OR. Si ce lien OR donne une valeur positive pour la relation ordinateur/utilisateur, la stratégie s'applique.

Avis : si plusieurs stratégies sont actives pour un objet, les stratégies individuelles sont groupées, en respectant néanmoins les règles décrites et fusionnées. En d'autres termes, les paramètres d'un objet peuvent être une combinaison de plusieurs stratégies différentes.

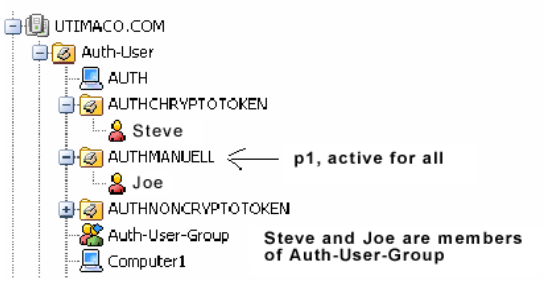
Un groupe peut avoir les paramètres d'activation suivants :

- **Activé**
  Une stratégie a été attribuée. Le groupe est affiché dans la zone d'activation de SafeGuard Management Center.
- **Non activé**
  Une stratégie a été attribuée. Le groupe ne se trouve pas dans la zone d'activation.

Si une stratégie est attribuée à un conteneur, le paramètre d'activation d'un groupe (activé) détermine si cette stratégie pour ce conteneur est incluse dans le calcul de la stratégie résultante.

Les stratégies héritées ne peuvent pas être contrôlées par ces activations. « Bloquer l'héritage de stratégie » doit être défini dans l'unité organisationnelle la plus locale pour annuler l'effet de la stratégie globale à cet endroit.

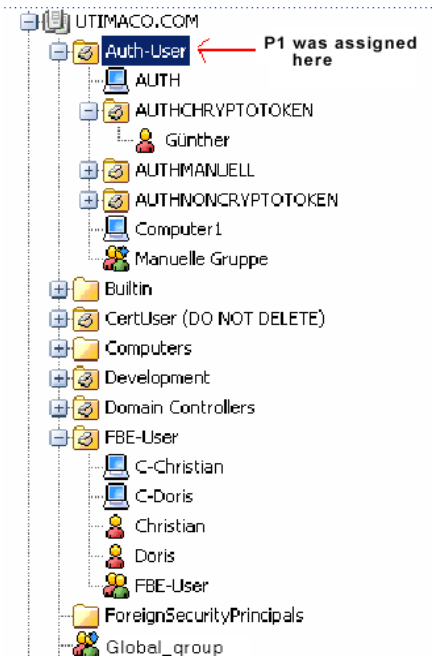
Exemple1 :



Il existe une attribution valide de la stratégie P1 pour le OU **AUTHMANUELL** et une activation pour le groupe **Auth-User-Group**. Emil et Gunther sont membres du groupe **Auth-User-Group**. Bien que l'utilisateur Gunther soit également membre du groupe **Auth-User-Group**, la stratégie P1 ne s'applique pas à lui, mais uniquement à l'utilisateur Emil. Comme il n'existe pas d'attribution valide de la stratégie P1 pour l'utilisateur Gunther (l'utilisateur Gunther n'appartient pas au OU **AUTHMANUELL**), l'activation du groupe **Auth-User-Group** n'a aucun effet sur lui.

Exemple 2

- Structure des AD comme sur la droite
- La stratégie P1 a été attribuée au OU `Auth-User` et n'est effective que pour le OU `Auth-User` et ses OU inférieurs.
- Pour les `Utilisateurs authentifiés` et les `Ordinateurs authentifiés`, la stratégie P1 **N'EST PAS activée**
- La stratégie P1 n'a été activée que pour le groupe global `Global_Group` (seul l'utilisateur `Gunther` est un membre de ce groupe. Le groupe `Global_Group` lui-même se trouve directement sous le nœud du domaine).



La stratégie P1 est effective pour l'utilisateur Gunther car il a reçu (indirectement) une attribution valide de la stratégie à partir du OU `Auth-User`. Cet exemple illustre que l'activation d'une stratégie peut s'effectuer n'importe où dans Active Directory. Ici, seul compte le fait qu'une attribution valide a été effectuée.

10.8.6 Paramètres de l'utilisateur ou du groupe

Les paramètres de stratégie pour les utilisateurs (paramètres illustrés en **noir** dans SafeGuard Management Center) sont prioritaires sur les paramètres de stratégie pour les ordinateurs (paramètres illustrés en **bleu** dans SafeGuard Management Center). Si les paramètres de l'utilisateur s'effectuent dans une stratégie pour les ordinateurs, ces paramètres seront remplacés par la stratégie pour l'utilisateur.

Avis : seuls les paramètres de l'utilisateur seront remplacés. Si une stratégie pour les utilisateurs comporte également des paramètres machine (paramètres affichés en **bleu**), ils ne seront pas remplacés par une stratégie d'utilisateur.
Exemple 1 :
si une longueur de mot de passe de 4 a été définie pour un groupe d'ordinateurs, et si la valeur 3 du même paramètre a été définie pour le groupe d'utilisateurs, un mot de passe de longueur 3 s'applique à cet utilisateur sur un ordinateur appartenant à ce groupe d'ordinateurs.
Exemple 2 :
Si un intervalle de connexion au serveur de 1 minute est défini pour un groupe d'utilisateurs, et si la valeur 3 est définie pour un groupe de machines,
la valeur 3 est utilisée car la valeur 1 minute est un paramètre machine ayant été défini dans une stratégie pour les utilisateurs.

10.8.7 Stratégies de chiffrement contradictoires

Deux stratégies - P1 et P2 - sont créées. Le chiffrement basé sur fichier de l'unité E:\ a été défini pour P1, et le chiffrement du volume de l'unité E:\ a été défini pour P2. P1 se voit attribuer le OU **FBE-User** et P2 le OU **VBE-User**.

Cas 1 : Un utilisateur du OU **FBE-User** se connecte le premier au client XP-100 (ordinateur du conteneur). Le chiffrement de l'unité E:\ est basé sur fichier. Si un utilisateur du OU **FBE-User** se connecte ensuite au client XP-100, le chiffrement de l'unité E:\ est basé sur le volume. Si les deux utilisateurs ont la même clé, tous deux peuvent accéder aux unités ou aux fichiers.

Cas 2 : Un utilisateur du OU **VBE-User** se connecte le premier à l'ordinateur XP-100 (ordinateur du conteneur). Le chiffrement de l'unité est basé sur le volume. À présent, si un utilisateur du OU **FBE-User** se connecte et a la même clé que des utilisateurs du OU **VBE-User**, le chiffrement de l'unité E:\ (le chiffrement du volume est conservé) sera basé sur fichier au sein du chiffrement du volume. Toutefois, si l'utilisateur du OU **FBE-User** n'a pas la même clé, il ne peut pas accéder à l'unité E:\.

10.8.8 Priorités au sein d'une attribution

La stratégie ayant la priorité la plus élevée (1) passe avant celle ayant une priorité inférieure au sein d'une attribution.

Avis : si une stratégie ayant une priorité inférieure mais ayant été désignée « Ne pas remplacer » est attribuée au même niveau qu'une stratégie d'un niveau supérieur, cette stratégie sera prioritaire en dépit de son niveau inférieur.

10.8.9 Priorités au sein d'un groupe

La stratégie ayant la priorité la plus élevée (1) passe avant celle ayant une priorité inférieure au sein d'un groupe.

10.8.10 Indicateurs d'état

La définition d'indicateurs d'état permet de changer les règles par défaut pour les stratégies.

- **Bloquer l'héritage de stratégie**

  Défini pour les conteneurs pour lesquels vous ne souhaitez pas que des stratégies de niveau supérieur s'appliquent (cliquez avec le bouton droit sur l'objet dans la fenêtre de navigation Propriétés).

- **Ne pas remplacer**

  Définie au cours de l'attribution, cette stratégie ne peut pas être remplacée par une autre.

Bloquer l'héritage de stratégie

Si vous ne souhaitez pas qu'un objet conteneur hérite d'une stratégie d'un objet plus élevé, sélectionnez « Bloquer l'héritage de stratégie » pour l'en empêcher. Si « Bloquer l'héritage de stratégie » a été sélectionné pour un objet conteneur, il ne sera pas affecté par les paramètres d'une stratégie d'un niveau supérieur (exception : « Ne pas remplacer » activé lorsqu'une stratégie a été attribuée).

Ne pas remplacer

Plus l'attribution de la stratégie « Ne pas remplacer » est éloignée de l'objet cible, plus cette stratégie a d'effet sur tous les objets conteneurs de niveau inférieur. Cela signifie qu'un conteneur de niveau supérieur soumis à « Ne pas remplacer » remplace les paramètres de stratégie d'un conteneur de niveau inférieur. Ainsi, par exemple il est possible de définir une stratégie de domaine dont les paramètres ne peuvent pas être remplacés, même si « Bloquer l'héritage de stratégie » a été défini pour une unité organisationnelle.

Avis : si une stratégie ayant une priorité inférieure mais ayant été désignée « Ne pas remplacer » est attribuée au même niveau qu'une stratégie d'un niveau supérieur, cette stratégie sera prioritaire en dépit de son niveau inférieur.

10.8.11 Paramètres de stratégie

Paramètres machine de relecture

Vous trouverez ce paramètre sous :
Éléments de stratégie > stratégie du type **Paramètres généraux** > **Chargement de paramètres** > **Mode de récursivité des stratégies**

Si vous sélectionnez « Paramètres machine de relecture » dans le champ **Mode de récursivité des stratégies** d'une stratégie du type Paramètres généraux et que la stratégie provient d'un ordinateur (« Paramètres machine de relecture » n'affecte pas les stratégies utilisateur), cette stratégie est relue à la fin de l'analyse. Ceci remplace ensuite les paramètres de l'utilisateur et les paramètres de la machine s'appliquent. Tous les paramètres de la machine hérités directement ou indirectement par la machine (y compris les stratégies qui n'ont pas été appliquées par le mode de récursivité des stratégies « Paramètres machine de relecture ») sont remplacés.

Ignorer l'utilisateur

Vous trouverez ce paramètre sous :
Éléments de stratégie > stratégie du type **Paramètres généraux** > **Chargement de paramètres** > **Mode de récursivité des stratégies**

Si vous sélectionnez « Ignorer l'utilisateur » pour une stratégie d'ordinateur dans le champ **Mode de récursivité des stratégies** d'une stratégie du type Paramètres généraux et que la stratégie provient d'une machine, seuls les paramètres de la machine sont analysés. Les paramètres de l'utilisateur ne sont pas analysés.

Aucun bouclage

Vous trouverez ce paramètre sous :
Éléments de stratégie > stratégie du type **Paramètres généraux** > **Chargement de paramètres** > **Mode de récursivité des stratégies**

Aucun bouclage décrit le comportement standard. Les stratégies de l'utilisateur sont prioritaires sur celles de l'ordinateur.

Analyse des paramètres « Ignorer l'utilisateur » et « Paramètres machine de relecture »

S'il existe des attributions de stratégies actives, les stratégies de la machine sont analysées et regroupées d'abord. Si, avec l'option Mode de récursivité des stratégies, ce regroupement de stratégies individuelles produit la valeur « Ignorer l'utilisateur », les stratégies qui auraient été fixées pour l'utilisateur ne sont pas analysées. Cela signifie que les mêmes stratégies s'appliquent à la fois pour l'utilisateur et pour la machine.

Si, lorsque les stratégies individuelles de la machine ont été regroupées, la valeur de l'attribut Mode de récursivité des stratégies est « Paramètres machine de relecture », les stratégies de l'utilisateur sont combinées à celles de la machine. Après le regroupement, les stratégies de la machine sont réécrites et, le cas échéant, remplacent les paramètres de stratégie de l'utilisateur. Si un paramètre est présent dans les deux stratégies, la valeur de la stratégie de la machine remplace celle de la stratégie de l'utilisateur.

Si le regroupement des stratégies individuelles de la machine produit la valeur par défaut (« Pas de mode de récursivité des stratégies »), les paramètres de l'utilisateur sont prioritaires par rapport à ceux de la machine.

Ordre d'exécution des stratégies

Ignorer l'utilisateur Ordinateurs

Paramètres machine de relecture Ordinateur -> Utilisateurs -> Ordinateur La première « exécution sur machine » est requise pour les stratégies qui sont écrites avant que la connexion utilisateur n'intervienne (par ex. image d'arrière-plan lors de la connexion).

Aucun bouclage (paramètre standard) : Ordinateur -> Utilisateur

10.8.12 Autres définitions

C'est l'origine d'une stratégie qui permet de déterminer s'il s'agit d'une stratégie d'utilisateur ou d'une stratégie de machine. Un objet de l'utilisateur « appelle » une stratégie d'utilisateur, et un ordinateur « appelle » une stratégie d'ordinateur. La même stratégie peut être une stratégie de machine ou d'utilisateur, selon le point de vue.

- **Stratégie de l'utilisateur**

  Toute stratégie fournie par l'utilisateur pour l'analyse. Si une stratégie est mise en œuvre via un seul utilisateur, les paramètres associés à la machine de cette stratégie ne sont pas appliqués, en d'autres termes les paramètres associés à l'ordinateur ne s'appliquent pas. Les valeurs par défaut s'appliquent.

- **Stratégie de l'ordinateur**

  Toute stratégie fournie par la machine pour l'analyse. Si une stratégie est mise en œuvre via un seul ordinateur, les paramètres spécifiques de l'utilisateur pour cette stratégie sont également appliqués. La stratégie de l'ordinateur représente par conséquent une stratégie « pour tous les utilisateurs ».

11 Utilisation de packages de configuration

Dans SafeGuard Management Center, vous pouvez créer les types de package de configuration suivants :

- **Package de configuration pour ordinateurs gérés**

  Les ordinateurs connectés à SafeGuard Enterprise Server reçoivent leurs stratégies via ce serveur. Pour garantir un bon fonctionnement une fois le logiciel SafeGuard Enterprise Client installé, vous devez créer un package de configuration pour les ordinateurs gérés et le déployer sur ceux-ci.

  Une fois la première configuration de l'ordinateur final effectuée par le biais du package de configuration, l'ordinateur reçoit des stratégies via le serveur SafeGuard Enterprise après que vous avez attribué celles-ci dans la zone **Utilisateurs & ordinateurs** de SafeGuard Management Center.

- **Package de configuration pour ordinateurs non gérés**

  Les ordinateurs non gérés ne sont connectés au serveur SafeGuard Enterprise à aucun moment, et fonctionnent en mode autonome. Ces ordinateurs reçoivent leurs stratégies par le biais de packages de configuration. Pour garantir un bon fonctionnement, vous devez créer un package de configuration contenant les groupes de stratégies appropriés, puis le distribuer sur les ordinateurs finaux via les mécanismes de distribution de l'entreprise. Dès que les paramètres de stratégie sont modifiés, de nouveaux packages de configuration doivent être créés et distribués aux ordinateurs finaux.

- **Package de configuration pour le serveur SafeGuard Enterprise**

  Pour garantir un bon fonctionnement, vous devez créer un package de configuration pour le serveur SafeGuard Enterprise qui définira la base de données et la connexion SSL, activera l'API de script, etc.

Pour obtenir une description détaillée de la création des différents types de package de configuration, consultez le manuel d'installation de SafeGuard Enterprise.

Remarque: Vérifiez votre réseau et vos ordinateurs à intervalles réguliers pour détecter les packages de configuration obsolètes ou non utilisés. De même, pour des raisons de sécurité, n'oubliez pas de les supprimer. Assurez-vous de toujours désinstaller les « anciens » packages de configuration avant d'installer tout nouveau package de configuration sur l'ordinateur/le serveur.

12 Options d'accès administratif sur les ordinateurs finaux

Afin de fournir un accès destiné aux tâches administratives après l'installation de SafeGuard Enterprise sur les ordinateurs finaux, SafeGuard Enterprise propose les options d'accès spécial suivantes :

- **Comptes de service pour la connexion Windows**

  Grâce aux comptes de service, les utilisateurs peuvent se connecter (connexion Windows) aux ordinateurs finaux après l'installation de SafeGuard Enterprise, sans avoir à activer l'authentification au démarrage et sans être ajoutés en tant qu'utilisateurs sur les ordinateurs. Les listes de comptes de service sont définies dans la zone **Stratégies** de SafeGuard Management Center et affectées aux ordinateurs finaux via des stratégies. Les utilisateurs figurant sur une liste de comptes de service sont considérés comme des utilisateurs invités lorsqu'ils se connectent à l'ordinateur final.

Remarque: Étant donné que les comptes de service sont particulièrement utiles durant la phase de déploiement d'une mise en œuvre, nous recommandons d'affecter des listes de comptes de service dès la création du package de configuration initiale SafeGuard Enterprise dans SafeGuard Management Center pour pouvoir configurer l'ordinateur final protégé par SafeGuard Enterprise après l'installation.

Pour des informations détaillées sur les comptes de service, reportez-vous à voir *Listes de comptes de service pour la connexion Windows*, à la page 92.

- **Comptes d'accès POA pour connexion POA sur des ordinateurs finaux non gérés protégés par SafeGuard Enterprise**

  Pour des ordinateurs finaux non gérés, c'est-à-dire des ordinateurs finaux fonctionnant en mode autonome, SafeGuard Enterprise propose des comptes d'accès POA. Les comptes d'accès POA sont des comptes locaux prédéfinis qui permettent aux utilisateurs de se connecter (connexion POA) à des ordinateurs finaux, une fois l'authentification au démarrage activée, pour effectuer des tâches administratives Les comptes sont définis dans la zone **Utilisateur & ordinateurs** de SafeGuard Management Center (nom d'utilisateur et mot de passe) et affectés aux ordinateurs finaux via des groupes d'accès POA inclus dans les packages de configuration.

  Pour des informations détaillées sur les comptes de service, reportez-vous à voir *Comptes d'accès POA pour la connexion POA sur des ordinateurs finaux non gérés*, à la page 98.

13 Listes de comptes de service pour la connexion Windows

Exemple de scénario type pour la plupart des mises en œuvre : une équipe de déploiement installe de nouveaux ordinateurs dans un environnement sur lequel SafeGuard Enterprise est installé. Pour des raisons d'installation ou de vérification, les opérateurs en charge du déploiement peuvent se connecter à leur ordinateur respectif avant que l'utilisateur final ne reçoive sa nouvelle machine et n'active l'authentification au démarrage.

Le scénario peut ainsi être le suivant :

1. SafeGuard Enterprise est installé sur un ordinateur final.
2. Après le redémarrage de l'ordinateur, l'opérateur en charge du déploiement se connecte.
3. L'opérateur en charge du déploiement est ajouté à l'authentification au démarrage, qui devient active. L'opérateur en charge du déploiement devient le propriétaire de l'ordinateur.

À la réception de son ordinateur, l'utilisateur final ne pourra pas se connecter au POA et doit effectuer une procédure Challenge/Réponse.

Pour éviter que ces opérations d'administration sur un ordinateur protégé par SafeGuard Enterprise n'activent l'authentification au démarrage et n'entraînent l'ajout sur l'ordinateur d'opérateurs en charge du déploiement en tant qu'utilisateurs et propriétaires d'ordinateurs, SafeGuard Enterprise offre la possibilité de créer des listes de comptes de service pour les ordinateurs protégés par SafeGuard Enterprise. Les utilisateurs figurant dans ces listes sont ainsi traités comme des utilisateurs invités de SafeGuard Enterprise.

Avec les comptes de service, le scénario est le suivant :

1. SafeGuard Enterprise est installé sur un ordinateur final.
2. Après le redémarrage de l'ordinateur, un opérateur en charge du déploiement et figurant sur une liste de comptes de service se connecte (connexion Windows).
3. D'après la liste de comptes de service appliquée à l'ordinateur, l'utilisateur est identifié comme un compte de service et traité comme utilisateur invité.

L'opérateur en charge du déploiement ne sera pas ajouté à POA et l'authentification au démarrage ne sera pas active. L'opérateur en charge du déploiement ne deviendra pas le propriétaire de l'ordinateur. L'utilisateur final peut se connecter et activer le POA.

Remarque: Étant donné que la fonctionnalité de liste de comptes de service est tout particulièrement utile durant la phase de déploiement d'une mise en œuvre, nous recommandons d'affecter des listes de comptes de service dès la création du package de configuration initiale SafeGuard Enterprise dans SafeGuard Management Center pour pouvoir configurer l'ordinateur final protégé par SafeGuard Enterprise après l'installation.

13.1 Création de listes de comptes de service et ajout d'utilisateurs

Pour créer des listes de comptes de service et ajouter des utilisateurs, procédez comme suit :

1. Cliquez sur **Stratégies** dans la zone de navigation.
2. Sélectionnez **Listes de comptes de service** dans la fenêtre de navigation de la stratégie.
3. Dans le menu contextuel de l'option **Listes de comptes de service**, cliquez sur **Nouveau > Liste de comptes de service**.
4. Entrez un nom pour la liste de comptes de service, puis cliquez sur **OK**.
5. Sélectionnez la nouvelle liste sous **Listes de comptes de service** dans la fenêtre de navigation de la stratégie.
6. Cliquez avec le bouton droit de la souris dans la zone d'action pour ouvrir le menu contextuel de la liste de comptes de service. Dans le menu contextuel, sélectionnez **Ajouter**.
7. Une nouvelle ligne utilisateur est ajoutée. Entrez le **Nom d'utilisateur** et le **Nom du domaine** dans les colonnes respectives, puis appuyez sur Entrée. Répétez cette étape pour ajouter d'autres utilisateurs.
8. Enregistrez vos modifications en cliquant sur l'icône **Enregistrer** de la barre d'outils.

La liste de comptes de service est à présent enregistrée et peut être sélectionnée dès lors que vous créez une stratégie.

13.2 Informations supplémentaires pour la saisie de noms d'utilisateur et de domaine

Il existe plusieurs méthodes servant à spécifier des utilisateurs dans les listes de comptes de service. Deux champs sont alors utilisés : **Nom d'utilisateur** et **Nom du domaine**(voir *Présentation des différentes combinaisons de connexion*, à la page 94. Par ailleurs, certaines restrictions s'appliquent concernant la saisie de ces champs (voir *Restrictions*, à la page 95).

13.2.1 Présentation des différentes combinaisons de connexion

Les deux champs séparés **Nom d'utilisateur** et **Nom du domaine** par entrée de liste offrent la souplesse nécessaire pour couvrir toutes les combinaisons disponibles de connexion, par exemple utilisateur@domaine ou domaine\utilisateur.

Pour gérer plusieurs combinaisons nom d'utilisateur/nom de domaine, vous pouvez utiliser les astérisques (*) comme caractères génériques. Une astérisque peut remplacer le premier signe, le dernier signe ou être le seul signe autorisé.

Par exemple :

- **Nom d'utilisateur :** Administrateur
- **Nom du domaine :** *

Cette combinaison indique tous les utilisateurs ayant pour nom d'utilisateur Administrateur et se connectant à un poste en local ou en réseau quel qu'il soit.

Le nom du domaine prédéfini [LOCALHOST] disponible dans la liste déroulante du champ **Nom du domaine** indique une connexion à n'importe quel poste de travail en local.

Par exemple :

- **Nom d'utilisateur** : "*admin"
- **Nom du domaine** : [LOCALHOST]

Cette combinaison indique tous les utilisateurs dont le nom d'utilisateur se termine par « admin » et se connectant à un poste en local quel qu'il soit.

En outre, les utilisateurs ont la possibilité de se connecter de plusieurs manières différentes, par exemple :

- utilisateur : test, domaine : masociété ou
- utilisateur : test, domaine : masociété.com.

Étant donné que les spécifications de domaine dans les listes de comptes de service ne sont pas automatiquement résolues, trois méthodes sont disponibles qui servent à indiquer correctement le domaine :

- Vous savez exactement comment l'utilisateur va se connecter et saisir le domaine en conséquence.

- Vous créez plusieurs entrées de liste de comptes de service.
- Vous utilisez les caractères génériques pour couvrir l'ensemble des cas (utilisateur : test, domaine : masociété*).

Remarque: Afin d'éviter les problèmes liés au fait que Windows peut utiliser des noms tronqués et non la même séquence de caractères, il est recommandé de saisir le NomComplet ou le nom Netbios, voire d'utiliser des caractères génériques.

13.2.2 Restrictions

Un astérisque ne peut remplacer que le premier signe, le dernier signe ou être le seul signe autorisé. Voici quelques exemples de chaînes valides et non valides concernant l'utilisation des astérisques :

- Exemples de chaînes valides : admin*, *, *strator, *minis*.
- Exemple de chaînes non valides : **, Admin*trator, Ad*minst*.

En outre, les restrictions suivantes s'appliquent :

- Le caractère ? n'est pas autorisé dans les noms de connexion utilisateur.
- Les caractères / \ [ ] : ; | = , + * ? < > " ne sont pas autorisés dans les noms de domaine.

13.3 Modification et suppression des listes de comptes de service

En tant que responsable de la sécurité possédant le droit **Modifier les listes de comptes de service**, vous pouvez modifier ou supprimer les listes de comptes de service à tout moment :

- Pour modifier une liste de comptes de service, double-cliquez dans la fenêtre de navigation de la stratégie. La liste de comptes de service s'ouvre et vous pouvez alors ajouter, supprimer ou modifier les noms d'utilisateur dans la liste.
- Pour supprimer une liste de comptes de service, sélectionnez-la dans la fenêtre de navigation de stratégie, ouvrez le menu contextuel, puis sélectionnez **Supprimer**.

13.4 Affectation d'une liste de comptes de service via une stratégie

Pour sélectionner et affecter une liste de comptes de services, procédez comme suit :

1. Créez une nouvelle stratégie du type **Authentification** ou sélectionnez-en une existante.
2. Sous **Options de connexion**, sélectionnez la liste de comptes de service requise dans la liste déroulante du champ **Liste de comptes de service**.

Remarque: Le paramètre par défaut de ce champ est **[Aucune liste]**, c'est-à-dire qu'aucune liste de comptes de service ne s'applique. Les opérateurs en charge du déploiement se connectant à l'ordinateur après l'installation de SafeGuard Enterprise ne seront ainsi pas traités comme des utilisateurs invités. Ils pourront activer l'authentification au démarrage et être ajoutés à l'ordinateur. Pour annuler l'affectation d'une liste de comptes de service, sélectionnez l'option **[Aucune liste]**.

3. Enregistrez vos modifications en cliquant sur l'icône Enregistrer de la barre d'outils.

Vous pouvez à présent transférer la stratégie sur l'ordinateur concerné et rendre les comptes de service disponibles sur l'ordinateur.

Remarque: Si vous sélectionnez des listes de comptes de service différentes dans des stratégies qui le sont tout autant et qui correspondent toutes au RSOP (Resulting Set of Policies, paramètre valide pour un ordinateur/groupe spécifique), la liste de comptes de service affectée à la dernière stratégie appliquée prendra le dessus sur toutes les listes de comptes de service précédemment assignées. Les listes de comptes de service ne seront pas fusionnées.

13.5 Transfert de la stratégie à l'ordinateur final

La fonctionnalité de liste de comptes de service se révèle tout particulièrement utile et importante durant l'installation initiale, au cours de la phase de déploiement d'une mise en œuvre. C'est pourquoi nous recommandons le transfert des paramètres de liste de comptes de service sur l'ordinateur final, sitôt l'installation effectuée. Pour rendre disponible la liste des comptes de service sur l'ordinateur final à ce moment précis, ajoutez une stratégie de type **Authentification** lors de la création du package de configuration initiale pour pouvoir configurer l'ordinateur final après l'installation.

Vous pouvez modifier à tout moment la liste des comptes de service. Ces modifications seront transférées sur l'ordinateur final par le biais du serveur, selon la procédure habituelle.

13.6 Connexion à un ordinateur final à l'aide d'un compte de service

Lors de la première connexion à Windows après réinitialisation de l'ordinateur, un utilisateur figurant sur une liste de comptes de service se connecte à la machine concernée en tant qu'utilisateur invité SafeGuard Enterprise. Cette première connexion Windows à la machine ne déclenche pas de procédure d'authentification au démarrage, de même qu'elle n'ajoute pas l'utilisateur à l'ordinateur. L'info-bulle de l'icône de la barre d'état système de SafeGuard Enterprise « Synchronisation utilisateur initiale terminée » ne s'affiche pas.

13.6.1 Affichage du statut du compte de service sur l'ordinateur final

Le statut de connexion de l'utilisateur invité est également disponible via l'icône de la barre d'état système. Pour plus d'informations sur l'icône de la barre d'état système, consultez l'aide de l'utilisateur de SafeGuard Enterprise, chapitre *Icône de la barre d'état système et info-bulle* (description du champ sur l'état de l'utilisateur).

13.7 Consignation des événements

Les actions accomplies concernant les listes de comptes de service sont signalées par les événements du journal suivants :

SafeGuard Management Center

- Liste de comptes de service <nom> créée
- Liste de comptes de service <nom> modifiée
- Liste de comptes de service <nom> supprimée

Ordinateur protégé par SafeGuard Enterprise

- Utilisateur Windows <nom domaine/utilisateur> connecté à <horodatage> sur le poste <nom domaine/poste de travail> avec un compte de service SGN.
- Nouvelle liste de comptes de service <nom> importée.
- Liste de comptes de service <nom> supprimée.

14 Comptes d'accès POA pour la connexion POA sur des ordinateurs finaux non gérés

Dans le cadre d'ordinateurs non gérés protégés par SafeGuard Enterprise, c'est-à-dire ceux fonctionnant en mode autonome, SafeGuard Enterprise propose des comptes d'accès POA. Une fois SafeGuard Enterprise installé et l'authentification au démarrage (POA) activée, vous devez pouvoir accéder aux ordinateurs finaux pour exécuter des tâches administratives. Grâce aux comptes d'accès POA, les utilisateurs peuvent se connecter aux ordinateurs finaux à partir de l'authentification au démarrage, pour exécuter des tâches administratives, sans avoir à lancer de procédure Challenge/Réponse. Il n'y a pas de connexion automatique à Windows. Les utilisateurs se connectant avec leurs comptes d'accès POA doivent se connecter à Windows avec leurs comptes Windows existants.

14.1 Création de comptes d'accès POA

Pour créer des comptes d'accès POA, procédez comme suit :

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs & ordinateurs**, sous **POA**, sélectionnez **Utilisateurs POA**.
3. Dans le menu contextuel des **Utilisateurs POA**, cliquez sur **Nouveau > Créer un utilisateur**.

La boîte de dialogue **Créer un utilisateur** s'affiche.

4. Dans le champ **Nom complet**, saisissez un nom, par exemple le nom de connexion du nouvel utilisateur POA.
5. Vous pouvez également entrer une description pour le nouvel utilisateur POA.
6. Saisissez un mot de passe pour le nouveau compte d'accès POA et confirmez-le.

Remarque: Pour améliorer la sécurité, le mot de passe doit respecter certaines exigences minimales de complexité, par exemple une longueur minimum de 8 caractères, un mélange de caractères numériques et alphanumériques, etc. Si le mot de passe saisi est trop court, un message d'avertissement s'affiche.

7. Cliquez sur **OK**.

Le nouveau compte d'accès POA a été créé et l'utilisateur POA (compte d'accès POA) s'affiche sous **Utilisateurs POA** dans la zone de navigation **Utilisateurs et ordinateurs**.

14.2 Modification du mot de passe d'un compte d'accès POA

Pour modifier le mot de passe d'un compte d'accès POA, procédez comme suit :

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs & ordinateurs**, sous **POA**, **Utilisateurs POA**, sélectionnez un utilisateur POA.
3. Dans le menu contextuel de cet utilisateur POA, sélectionnez **Propriétés**.

La boîte de dialogue Propriétés de l'utilisateur POA s'affiche.

4. Dans l'onglet **Général**, sous **Mot de passe utilisateur**, saisissez le nouveau mot de passe et confirmez-le.
5. Cliquez sur **OK**.

Le nouveau mot de passe est attribué au compte d'accès POA correspondant.

14.3 Suppression de comptes d'accès POA

Pour supprimer des comptes d'accès POA, procédez comme suit :

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs & ordinateurs**, sous **POA**, **Utilisateurs POA**, sélectionnez un compte d'accès POA.
3. Cliquez avec le bouton droit de la souris sur le compte d'accès POA et sélectionnez **Supprimer** dans le menu contextuel.

Le compte d'accès POA (utilisateur POA) est supprimé et n'apparaît plus dans la fenêtre de navigation **Utilisateurs & ordinateurs**.

Remarque: Si l'utilisateur appartient à un ou plusieurs groupes POA, le compte d'accès POA sera également supprimé de ces groupes. Le compte d'accès POA reste cependant disponible sur l'ordinateur final jusqu'à ce qu'un nouveau package de configuration soit créé et attribué. Pour en savoir plus sur les groupes POA, reportez-vous à voir *Création de groupes de comptes d'accès POA*, à la page 100. Pour en savoir plus sur la modification des attributions des comptes d'accès POA, reportez-vous à voir *Modification des attributions de comptes d'accès POA sur les ordinateurs finaux*, à la page 103.

14.4 Création de groupes de comptes d'accès POA

Pour pouvoir attribuer des comptes d'accès POA aux ordinateurs finaux via des packages de configuration, les comptes doivent être organisés par groupes. Lors de la création de packages de configuration, vous pouvez sélectionner un groupe de comptes d'accès POA à attribuer.

Pour créer des groupes de comptes d'accès POA, procédez comme suit :

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs**.
2. Dans la zone de navigation **Utilisateurs & ordinateurs**, sous **POA**, sélectionnez **Groupes POA**.
3. Dans le menu contextuel des **Groupes POA**, cliquez sur **Nouveau** > **Créer un groupe**.

La boîte de dialogue **Créer un groupe** s'affiche.

4. Dans le champ **Nom complet**, saisissez le nom du nouveau groupe POA.
5. Vous pouvez également entrer une description pour le nouveau groupe POA.
6. Cliquez sur **OK**.

Le nouveau groupe de comptes d'accès POA a été créé et est affiché sous **Groupes POA** dans la zone de navigation **Utilisateurs & ordinateurs**. Vous pouvez maintenant ajouter des utilisateurs (comptes d'accès POA) au groupe de comptes d'accès POA.

14.5 Ajout de comptes aux groupes de comptes d'accès POA

Pour ajouter des utilisateurs (comptes d'accès POA) aux groupes de comptes d'accès POA, procédez comme suit :

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs & ordinateurs**, sous **POA**, **Groupe POA**, sélectionnez un groupe POA.

Dans la zone d'action de SafeGuard Management Center, sur la droite, l'onglet **Membres** s'affiche.

3. Dans la barre d'outils de SafeGuard Management Center, cliquez sur l'icône **Ajouter** (signe « + » vert).

La boîte de dialogue **Sélectionner un objet membre** s'affiche.

4. Sélectionnez l'utilisateur (compte d'accès POA) que vous souhaitez ajouter au groupe.
5. Cliquez sur **OK**.

Le compte d'accès POA est ajouté au groupe, puis affiché dans l'onglet **Membres**.

Remarque: Vous pouvez également ajouter des comptes aux groupes en sélectionnant l'utilisateur POA (compte d'accès POA) dans la fenêtre de navigation et en exécutant les étapes décrites ci-dessus. Avec cette approche, l'onglet **Membre de** s'affiche dans la zone d'action une fois l'utilisateur sélectionné. Cet onglet affiche les groupes auxquels l'utilisateur a été attribué. Le flux de travail de base reste le même.

14.6 Suppression de membres des groupes de comptes d'accès POA

Pour supprimer des membres (comptes d'accès POA) des groupes de comptes d'accès POA, procédez comme suit :

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs & ordinateurs**, sous **POA**, **Groupe POA**, sélectionnez un groupe POA.

Dans la zone d'action de SafeGuard Management Center, sur la droite, l'onglet **Membres** s'affiche.

3. Sélectionnez l'utilisateur que vous souhaitez supprimer du groupe.
4. Dans la barre d'outils de SafeGuard Management Center, cliquez sur l'icône **Supprimer** (croix rouge).

L'utilisateur est supprimé du groupe.

Remarque: Vous pouvez également supprimer des membres des groupes en sélectionnant l'utilisateur POA (compte d'accès POA) dans la fenêtre de navigation et en exécutant les étapes décrites ci-dessus. Avec cette approche, l'onglet **Membre de** s'affiche dans la zone d'action une fois l'utilisateur sélectionné. Cet onglet affiche les groupes auxquels l'utilisateur a été attribué. Le flux de travail de base reste le même.

14.7 Attribution de comptes d'accès POA aux ordinateurs finaux

Pour attribuer des groupes de comptes d'accès POA à des ordinateurs finaux via des packages de configuration, procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Outil de package de configuration** dans le menu **Outils**.
2. Sélectionnez un package de configuration existant ou créez-en un nouveau.
3. Spécifiez un **Groupe POA** préalablement créé dans la zone **Utilisateurs & ordinateurs** de SafeGuard Management Center qui sera appliqué aux ordinateurs.

   Le paramètre par défaut pour le groupe POA est **Aucun groupe**.

   Vous pouvez également sélectionner un groupe vide par défaut. Ce groupe peut être utilisé pour supprimer les attributions de groupes de comptes d'accès POA sur les ordinateurs finaux. Pour plus d'informations, reportez-vous à voir *Suppression de comptes d'accès POA des ordinateurs finaux*, à la page 102.
4. Spécifiez un chemin de sortie pour le fichier MSI.
5. Cliquez sur **Créer un MSI client autonome**.
6. Déployez le fichier MSI sur les ordinateurs finaux.

L'installation du fichier MSI entraîne l'ajout des utilisateurs (comptes d'accès POA) inclus dans le groupe au POA sur les ordinateurs finaux. Les comptes d'accès POA sont disponibles pour la connexion POA.

14.8 Suppression de comptes d'accès POA des ordinateurs finaux

Les comptes d'accès POA peuvent être supprimés des ordinateurs finaux en leur attribuant un groupe de comptes d'accès POA vide. Procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Outil de package de configuration** dans le menu **Outils**.
2. Sélectionnez un package de configuration existant ou créez-en un nouveau.
3. Spécifiez un **Groupe POA** vide créé préalablement dans la zone **Utilisateurs** de SafeGuard Management Center, ou sélectionnez le groupe POA vide fourni dans l'**Outil de package de configuration**.
4. Spécifiez un chemin de sortie pour le fichier MSI.

5. Cliquez sur **Créer un MSI client autonome**.
6. Déployez le fichier MSI sur les ordinateurs finaux.

L'installation du fichier MSI entraîne la suppression de tous les comptes d'accès POA des ordinateurs finaux. Tous les utilisateurs concernés sont donc supprimés de l'authentification au démarrage.

14.9 Modification des attributions de comptes d'accès POA sur les ordinateurs finaux

Pour modifier l'attribution des comptes d'accès POA sur les ordinateurs finaux, procédez comme suit :

1. Créez un nouveau groupe de comptes d'accès POA ou modifiez-en un existant.
2. Créez un nouveau package de configuration, puis sélectionnez un groupe de comptes d'accès POA existant ou celui que vous venez de créer.

Le nouveau groupe de comptes d'accès POA est disponible sur l'ordinateur final. Tous les utilisateurs inclus sont ajoutés à l'authentification au démarrage. Le nouveau groupe remplace le précédent. Les groupes de comptes d'accès POA ne sont pas fusionnés.

14.10 Connexion à un ordinateur final à l'aide d'un compte d'accès POA

Pour vous connecter à l'aide d'un compte d'accès POA, procédez comme suit :

1. Mettez l'ordinateur sous tension.

La boîte de dialogue de connexion de l'authentification au démarrage s'affiche.

2. Saisissez le **Nom d'utilisateur** et le **Mot de passe** du compte d'accès POA prédéfini.

Vous n'êtes pas connecté à Windows automatiquement. Par conséquent, la boîte de dialogue de connexion Windows s'affiche.

3. Dans le champ **Domaine**, sélectionnez le domaine **<POA>**.
4. Connectez-vous à Windows à l'aide de votre compte utilisateur Windows existant.

15 Stratégies de sécurité

Les stratégies de SafeGuard Enterprise comportent tous les paramètres devant être actifs pour mettre en œuvre une stratégie de sécurité à l'échelle de l'entreprise sur les ordinateurs finaux.

Les stratégies de SafeGuard Enterprise peuvent comporter des paramètres pour les domaines suivants (types de stratégies) :

- **Paramètres généraux**
  Contient, par exemple, des paramètres de taux de transfert, d'images d'arrière-plan, etc.
- **Authentification**
  Contient des paramètres de mode de connexion, verrouillage de périphérique, etc.
- **Codes PIN**
  Définit la configuration minimale des codes PIN utilisés.
- **Mots de passe**
  Définit la configuration minimale des mots de passe utilisés.
- **Passphrases**
  Définit la configuration minimale des passphrases utilisées. Les passphrases sont utilisées pour un échange de données sécurisé avec SafeGuard Data Exchange lors de la génération d'une clé.
- **Protection du périphérique**
  Contient les paramètres de chiffrement basé sur volume ou sur fichier (notamment les paramètres de SafeGuard Data Exchange et de SafeGuard Portable) : algorithmes, clés, lecteurs sur lesquels les données doivent être chiffrées, etc.
- **Paramètres de machine spécifiques**
  Contient les paramètres d'authentification au démarrage (activer/désactiver), d'éveil par appel réseau sécurisé, d'options d'affichage, etc.
- **Consignation**
  Définit les événements à consigner et leurs destinations de sortie.
- **Protection de la configuration**
  Contient des paramètres (autoriser/bloquer) d'utilisation des ports et des périphériques (PDA, supports amovibles, imprimantes, etc.).

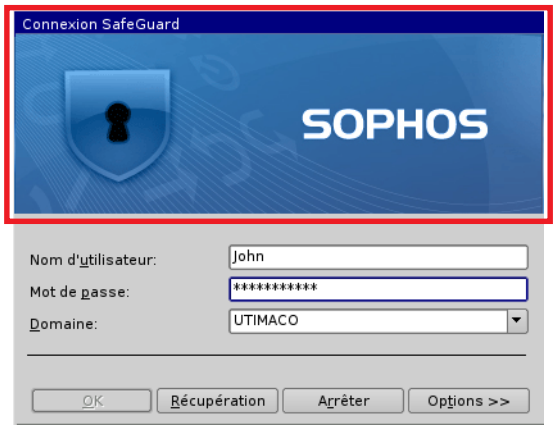
15.1 Paramètres généraux

Paramètre de stratégie	Explication
CHARGEMENT DE PARAMÈTRES	
Mode de récursivité des stratégies	**Paramètres de relecture de la machine** Si « Paramètres de relecture de la machine » est sélectionné pour une stratégie incluse dans le champ **Mode de récursivité des stratégies** et si la stratégie provient d'une machine (le paramètre « Répéter machine » d'une stratégie d'utilisateur n'entraîne aucun effet), cette stratégie est mise en œuvre une nouvelle fois à la fin. Ceci remplace ensuite les paramètres de l'utilisateur et les paramètres de la machine s'appliquent. **Ignorer l'utilisateur** Si vous sélectionnez « Ignorer l'utilisateur » pour une stratégie (stratégie de machine) dans le champ **Mode de récursivité des stratégies**, et si la stratégie provient d'une machine, seuls les paramètres de la machine sont analysés. Les paramètres de l'utilisateur ne sont pas analysés. **Aucun bouclage** Aucun bouclage est le comportement standard dans lequel les stratégies de l'utilisateur sont prioritaires sur celles de la machine. **Comment les paramètres « Ignorer l'utilisateur » et « Paramètres de relecture de la machine » sont-ils analysés ?** S'il existe des attributions de stratégies actives, les stratégies de la machine sont analysées et regroupées d'abord. Si le regroupement des différentes stratégies se traduit par l'attribut « Ignorer l'utilisateur » dans l'option Mode de récursivité des stratégies, les stratégies qui auraient été appliquées pour l'utilisateur ne sont plus analysées. Cela signifie que les mêmes stratégies s'appliquent à l'utilisateur et à la machine. Si la valeur « Paramètres de relecture de la machine » est appliquée dans le cas du mode de récursivité des stratégies, lorsque les stratégies individuelles de la machine ont été regroupées, les stratégies de l'utilisateur sont ensuite combinées à celles de la machine. Après le regroupement, les stratégies de la machine sont réécrites et remplacent les paramètres de stratégie de l'utilisateur. Cela signifie que, si un paramètre est présent dans les deux stratégies, la valeur de la stratégie de la machine remplace celle de la stratégie de l'utilisateur. Si le regroupement des stratégies individuelles de la machine produit la valeur standard, ce qui suit s'applique : Les paramètres de l'utilisateur sont prioritaires sur ceux de la machine.

Paramètre de stratégie	Explication
TAUX DE TRANSFERT	
Intervalle de connexion au serveur (min)	Détermine la période, en minutes, après laquelle un client SafeGuard Enterprise envoie une demande de stratégie (modifications) au serveur SafeGuard Enterprise. **Avis :** pour éviter qu'un grand nombre de clients ne contactent le serveur simultanément, la communication s'effectue toujours dans une période de +/- 50 % de l'intervalle de connexion défini. Exemple : le paramètre « 90 minutes » se traduit par une période de communication entre le client et le serveur de 45 à 135 minutes.
CONSIGNATION	
Commentaires après plusieurs événements	Le système de consignation mis en œuvre en tant que service Win32 « SGM LogPlayer » recueille les entrées du journal générées par SafeGuard Enterprise pour la base de données centrale et les stocke dans les fichiers journaux locaux. Elles sont stockées dans le cache local dans le répertoire « Auditing\SGMTransLog ». Ces fichiers sont transférés au mécanisme de transport qui les envoie ensuite à la base de données via le serveur SGN. Le transfert s'effectue dès que le mécanisme de transport a réussi à créer une connexion au serveur. La taille du fichier journal a donc tendance à augmenter jusqu'à ce qu'une connexion ait été établie. Pour limiter la taille de chaque fichier journal, il est possible de spécifier un nombre maximal d'entrées du journal dans la stratégie. Lorsque le nombre d'entrées prédéfini a été atteint, le système de consignation place le fichier journal dans la file d'attente de transport du serveur SGN et démarre un nouveau fichier journal.
PERSONNALISATION	
Langue utilisée sur le client	Détermine la langue dans laquelle les paramètres de SafeGuard Enterprise sont affichés sur l'ordinateur final : Outre les langues prises en charge, les utilisateurs peuvent sélectionner le paramètre de langue du système d'exploitation de l'ordinateur.

Paramètre de stratégie	Explication
RÉCUPÉRATION DE LA CONNEXION	
Activer la récupération de connexion après la corruption du cache local Windows	Le cache local Windows représente le point de départ et de fin de l'échange de données entre l'ordinateur final et le serveur. Il stocke la totalité des clés, stratégies, certificats utilisateur et fichiers d'audit. Toutes les données stockées dans le cache local sont signées et ne peuvent être modifiées manuellement. La récupération de connexion est désactivée par défaut. En d'autres termes, le cache local Windows sera restauré automatiquement à partir de sa sauvegarde. Aucune procédure de Challenge/Réponse n'est donc requise pour réparer le cache local Windows. Si le cache local Windows doit être réparé explicitement via une procédure de Challenge/Réponse, définissez ce champ sur « OUI ».
Activer Local Self Help	
Activer Local Self Help	Détermine si les utilisateurs sont autorisés à se connecter à leurs ordinateurs via Local Self Help en cas d'oubli de leur mot de passe. Grâce à Local Self Help, l'utilisateur peut se connecter en répondant à un nombre spécifique de questions prédéfinies dans l'authentification au démarrage. Ainsi, en cas d'urgence, l'utilisateur peut de nouveau accéder à son ordinateur même si aucune connexion téléphonique ou Internet n'est disponible. Une procédure Challenge/Réponse n'est pas nécessaire dans ce cas. Local Self Help permet de réduire les interventions et coûts relatifs au support. **AVIS :** La connexion automatique à Windows doit être activée pour que l'utilisateur puisse utiliser Local Self Help. Dans le cas contraire, Local Self Help ne fonctionne pas.
Longueur minimale des réponses	Dans ce champ, définissez la longueur minimale (en caractères) des réponses à enregistrer pour Local Self Help sur l'ordinateur final.
Texte de bienvenue sous Windows	Dans ce champ, vous pouvez spécifier le texte d'informations à afficher dans la première boîte de dialogue au démarrage de l'assistant de Local Self Help sur l'ordinateur final. Avant de pouvoir spécifier le texte ici, il doit être créé et enregistré.

Paramètre de stratégie	Explication
L'utilisateur peut définir des questions personnalisées	En tant que responsable de la sécurité, vous pouvez définir de manière centralisée les questions auxquelles répondre et les distribuer sur l'ordinateur final à l'aide de la stratégie. Vous pouvez cependant également accorder aux utilisateurs le droit de définir des questions personnalisées. Pour autoriser les utilisateurs à définir des questions personnalisées, sélectionnez **Oui** dans ce champ.
Challenge / Réponse (C/R)	
Activer la récupération de la connexion (via C/R)	Détermine si un utilisateur est autorisé à générer un challenge dans l'authentification au démarrage (POA) afin de pouvoir accéder de nouveau à son ordinateur via une procédure Challenge/Réponse. **OUI :** L'utilisateur est autorisé à générer un challenge. Dans ce cas, l'utilisateur peut de nouveau accéder à son ordinateur via une procédure C/R en cas d'urgence. **NON :** L'utilisateur n'est pas autorisé à générer un challenge. Dans ce cas, l'utilisateur ne peut pas exécuter une procédure C/R pour accéder de nouveau à son ordinateur en cas d'urgence.
Autoriser la connexion Windows automatique	Permet à l'utilisateur de se connecter automatiquement à Windows après s'être authentifié, en utilisant la procédure challenge/réponse. **OUI :** l'utilisateur est automatiquement connecté à Windows. **NON :** l'écran de connexion Windows apparaît. **Étude de cas :** Un utilisateur a oublié son mot de passe. Après la procédure de Challenge/Réponse, SafeGuard Enterprise connecte l'utilisateur à l'ordinateur sans mot de passe SGN. Dans ce cas, la connexion automatique à Windows est désactivée et l'écran de connexion Windows s'affiche. L'utilisateur ne peut pas se connecter car il ne connaît pas le mot de passe SGN (= mot de passe Windows). « OUI » autorise la connexion automatique et l'utilisateur peut continuer à partir de l'écran de connexion de Windows.
Texte d'informations	Affiche un texte d'informations lorsque l'on appuie sur le bouton **Challenge** dans POA. Les textes d'information peuvent inclure par ex. « Contactez le bureau de support en appelant le 01234-56789. » Avant d'insérer un texte ici, vous devez le créer sous forme de fichier texte dans la **zone de navigation de stratégie** sous **Texte d'informations**.

Paramètre de stratégie	Explication
IMAGES	
	Condition préalable : les nouvelles images doivent être enregistrées dans la **zone de navigation de stratégie** de SafeGuard Management Center sous **Images**. Les images ne sont disponibles qu'une fois enregistrées. Formats pris en charge : .BMP, PNG, JPEG.
Image d'arrière-plan dans POA	Remplace l'image bitmap bleue d'arrière-plan par l'écran SafeGuard pour l'arrière-plan que vous avez sélectionné. Par exemple, les clients peuvent utiliser le logo de l'entreprise dans POA et lors de la connexion de Windows. Taille de fichier maximum pour toutes les images bitmap d'arrière-plan : 500 Ko Résolution : 1024 x 768 (mode VESA) Couleurs : illimitées
Image d'arrière-plan dans POA (faible résolution)	Résolution : 640 x 480 (mode VGA) Couleurs : 16 couleurs
Image de connexion dans POA Image de connexion dans POA (faible résolution)	Change l'image bitmap de SafeGuard Enterprise affichée dans la boîte de dialogue de connexion à POA. Par exemple, le logo de l'entreprise peut être affiché dans cette boîte de dialogue. Résolution : 413 x 140 pixels Couleurs : illimitées. Résolution : 413 x 140 pixels Couleurs : 16 

15.2 Authentification

La manière dont les utilisateurs se connectent à leur poste de travail (avec ou sans clé cryptographique) est déterminée dans une stratégie de type **Authentification**.

Paramètre de stratégie	Explication
ACCÈS	
Les utilisateurs peuvent bouter à partir du disque dur uniquement	Détermine si les utilisateurs peuvent démarrer le PC à partir du disque dur et/ou d'un autre support. **OUI :** les utilisateurs peuvent bouter à partir du disque dur uniquement. L'Authentification au démarrage (POA) n'offre pas la possibilité de démarrer le PC avec une disquette ou un autre support externe. **NON :** les utilisateurs peuvent démarrer le PC à partir du disque dur, d'une disquette ou d'un support externe (USB, CD, etc.).
OPTIONS DE CONNEXION	
Mode de connexion	Détermine comment un utilisateur doit s'authentifier dans POA. ■ **ID utilisateur/Mot de passe** L'utilisateur ne peut pas se connecter avec une clé cryptographique. La connexion doit s'effectuer par l'intermédiaire du nom d'utilisateur et du mot de passe dans POA. ■ **Carte à puce** L'utilisateur ne peut se connecter dans POA qu'avec une clé cryptographique ou une carte à puce. Ce processus offre un niveau de sécurité plus élevé. L'utilisateur doit insérer sa clé lors de la connexion. L'identité de l'utilisateur est vérifiée par la possession de la clé et la présentation du code PIN. Après la saisie d'un code PIN correct, SafeGuard Enterprise lit automatiquement les données pour la connexion de l'utilisateur.

Paramètre de stratégie	Explication
	Avis : lorsque ce processus de connexion a été sélectionné, les utilisateurs ne peuvent se connecter qu'en utilisant une clé générée préalablement. Ce paramètre ne s'applique qu'à Windows XP. Il est possible de combiner les paramètres ci-dessus. Pour vérifier si la connexion fonctionne en utilisant une clé cryptographique, sélectionnez d'abord les deux paramètres. Ne désélectionnez le mode de connexion **ID utilisateur/Mot de passe** que si l'authentification avec la clé cryptographique a réussi. ■ **Empreinte digitale** Sélectionnez ce paramètre pour permettre la connexion à l'aide du lecteur d'empreintes digitales Lenovo. Les utilisateurs auxquels cette stratégie s'applique peuvent alors se connecter à l'aide d'une empreinte digitale ou d'un nom d'utilisateur et d'un mot de passe. Cette procédure offre le niveau de sécurité maximum. Lors de la connexion, l'utilisateur fait glisser son doigt sur le lecteur d'empreintes digitales. Lorsque l'empreinte digitale est correctement reconnue, le processus d'authentification au démarrage lit les informations d'identification de l'utilisateur et connecte l'utilisateur à l'authentification au démarrage. Le système transfère alors les informations d'identification vers Windows et connecte l'utilisateur à l'ordinateur. **Avis :** Après avoir sélectionné cette procédure de connexion, l'utilisateur peut se connecter uniquement à l'aide d'une empreinte digitale préenregistrée ou d'un nom d'utilisateur et d'un mot de passe. Vous ne pouvez pas utiliser conjointement les procédures de connexion par clé cryptographique et par empreinte digitale sur le même ordinateur.

Paramètre de stratégie	Explication
Options de connexion à l'aide d'une carte à puce	Détermine le type de clé cryptographique ou de carte à puce à utiliser sur le PC de l'utilisateur. ■ **Non cryptographique :** Authentification à POA et Windows basée sur les informations d'identification utilisateur. ■ **Kerberos :** Authentification basée sur les informations d'identification utilisateur à POA et Windows. Le SO émet un certificat dans une infrastructure de clé publique (PKI) et la stocke sur la clé cryptographique. Ce certificat est importé sous forme de certificat utilisateur dans la base de données SafeGuard Enterprise. Si un certificat généré automatiquement existe déjà dans une base de données, il est remplacé par le certificat importé. **Remarque :** avec les clés cryptographiques/cartes à puce prises en charge par Kerberos, aucune procédure Challenge/Réponse n'est possible car aucune information d'identification utilisateur utilisable pour une procédure Challenge/Réponse n'est fournie dans POA.
Code PIN utilisé pour la connexion automatique avec une carte à puce	Spécifiez un code PIN par défaut pour autoriser la connexion automatique de l'utilisateur à l'authentification au démarrage à l'aide d'une clé cryptographique ou d'une carte à puce. L'utilisateur doit insérer sa clé lors de la connexion et est orienté vers l'authentification au démarrage. Windows démarre. Il n'est pas nécessaire de suivre les règles relatives au code PIN. **Avis :** ■ Cette option n'est disponible que si vous sélectionnez **Carte à puce** comme **mode de connexion**. ■ Si cette option est activée, **Authentification automatique à Windows** doit être défini sur **Désactiver l'authentification automatique à Windows**.

Paramètre de stratégie	Explication
Afficher des connexions en échec pour cet utilisateur	Affiche (paramètre : OUI) après la connexion POA et Windows une boîte de dialogue indiquant des informations relatives au dernier échec de connexion (nom d'utilisateur/date/heure).
Afficher la dernière connexion utilisateur	Affiche (paramètre : OUI) après la connexion POA et Windows une boîte de dialogue indiquant des informations relatives à ■ la dernière connexion ayant réussi (nom d'utilisateur/date/heure) ; ■ les dernières informations d'identification de l'utilisateur connecté.
Désactiver la « déconnexion forcée » dans le verrouillage du poste de travail	Si des utilisateurs veulent quitter l'ordinateur final pendant une courte durée, ils peuvent cliquer sur **Verrouiller le poste de travail** pour empêcher d'autres utilisateurs d'utiliser l'ordinateur et le déverrouiller avec le mot de passe utilisateur. Si cette option est définie sur NON, l'utilisateur ayant verrouillé l'ordinateur ainsi qu'un administrateur peuvent le déverrouiller. Si un administrateur déverrouille l'ordinateur, l'utilisateur actuellement connecté est automatiquement déconnecté. La définition de ce champ sur OUI change ce comportement. Dans ce cas, seul l'utilisateur peut déverrouiller l'ordinateur. L'administrateur ne peut pas le déverrouiller et l'utilisateur ne se trouve pas automatiquement déconnecté. Avis : ce paramètre ne prend effet que sous Windows XP.
Activer la présélection utilisateur/ domaine	**OUI :** POA enregistre les nom d'utilisateur et domaine du dernier utilisateur connecté. Il n'est donc pas nécessaire que les utilisateurs saisissent leur nom d'utilisateur chaque fois qu'ils se connectent. **NON :** POA n'enregistre pas les nom d'utilisateur et domaine du dernier utilisateur connecté.

Paramètre de stratégie	Explication
Connexion automatique vers Windows	**Avis :** pour que l'utilisateur puisse autoriser à d'autres utilisateurs d'accéder à son ordinateur, il doit pouvoir désactiver l'authentification automatique à Windows. ■ **Laisser l'utilisateur choisir** L'utilisateur peut choisir en activant/désactivant cette option dans la boîte de dialogue de connexion POA d'exécuter ou non la connexion automatique à Windows. ■ **Appliquer l'authentification automatique à Windows** L'utilisateur se connecte toujours automatiquement à Windows. ■ **Désactiver l'authentification automatique à Windows** Après la connexion POA, la boîte de dialogue de connexion Windows s'affiche. L'utilisateur doit se connecter manuellement à Windows.
Liste de comptes de service	Pour éviter que les opérations d'administration sur un ordinateur protégé par SafeGuard Enterprise n'activent l'authentification au démarrage et n'entraînent l'ajout des opérateurs en charge du déploiement comme autant d'utilisateurs possibles de l'ordinateur, SafeGuard Enterprise offre la possibilité de créer des listes de comptes de service pour les ordinateurs finaux SafeGuard Enterprise. Les utilisateurs figurant dans ces listes sont ainsi traités comme des utilisateurs invités de SafeGuard Enterprise. Avant de sélectionner une liste, vous devez créer les listes dans la zone de navigation **Stratégies** sous **Listes de comptes de service**.

Paramètre de stratégie	Explication
Options BitLocker	
Mode de connexion BitLocker	Vous pouvez choisir le mode de connexion BitLocker parmi les options suivantes. ■ **TPM :** la clé de connexion est stockée sur la puce du TPM. ■ **TPM + PIN :** la clé de connexion est stockée sur la puce du TPM et un code PIN est également nécessaire pour la connexion. Les paramètres du code PIN sont fournis sous le code PIN et le mot de passe. ■ **Carte mémoire USB :** la clé de connexion est stockée sur une clé USB. ■ **TPM + carte mémoire USB :** la clé de connexion est stockée sur la puce du TPM et sur une clé USB. La connexion peut s'effectuer avec la puce du TPM ou la clé USB.
Mode de connexion de secours BitLocker	En cas d'échec de connexion, SafeGuard Enterprise permet la connexion avec une clé USB comme mécanisme de secours ou génère un message d'erreur. **Avis :** si vous sélectionnez *Carte mémoire USB* comme mode de connexion, cette option n'est pas proposée.

Paramètre de stratégie	Explication
Profil de validation de plate-forme TPM	Si un TPM est détecté sur l'ordinateur final, le type de profil de validation de plate-forme TPM à utiliser peut être configuré. Le profil de validation de plate-forme TPM spécifie les mesures utilisées pour protéger les clés de chiffrement pour BitLocker. Un profil de validation de plate-forme consiste en un jeu d'indices PCR (Platform Configuration Register). Microsoft recommande l'utilisation du profil de validation de plate-forme TPM par défaut sous Windows Vista qui protège les éléments suivants : ■ Clé de chiffrement contre tout changement du CRTM (Core Root of Trust of Measurement), BIOS et des extensions de plate-forme (PCR 0). ■ Code ROM d'option (PCR 2). ■ Code MBR (Master Boot Record) (PCR 4). ■ Secteur d'initialisation NTFS (PCR 8). ■ Code d'initialisation NTFS (PCR 9). ■ Gestionnaire d'initialisation (PCR 10). ■ Contrôle d'accès DE BitLocker (PCR 11). **Avis :** cette option n'est disponible que si vous sélectionnez *TPM* comme mode de connexion. Cette option n'est pas proposée si *Carte mémoire USB* est le mode de connexion sélectionné. Pour plus d'informations sur le profil de validation TPM, suivez le lien ci-dessous : *http://msdn2.microsoft.com/en-us/library/aa376469.aspx*

Paramètre de stratégie	Explication
ÉCHECS DE CONNEXION	
Nbre maximum d'échecs de connexion	Détermine le nombre de tentatives de connexion d'un utilisateur avec un nom d'utilisateur ou un mot de passe non valide. Par exemple, après trois tentatives successives de saisie d'un nom d'utilisateur ou d'un mot de passe incorrect, une quatrième tentative déclenche le paramètre « Réaction aux échecs de connexion ».
Messages d'échec de connexion dans l'authentification au démarrage (POA)	Définit le niveau de détail des messages d'échec de connexion : ■ Standard : affiche une brève description. ■ Détaillé : affiche des informations plus détaillées.
Réaction aux échecs de connexion	
Verrouiller la machine	Détermine si le PC est verrouillé après des tentatives de connexion incorrectes. Le verrouillage de l'ordinateur peut être levé par un administrateur qui doit réinitialiser le PC et se connecter. Tenez également compte du verrouillage utilisateur Windows dans ce contexte.
OPTIONS DE CARTE À PUCE	
Action si le statut de connexion à la carte à puce est perdu	Définit le comportement après suppression de la clé cryptographique de l'ordinateur : Les actions possibles sont les suivantes : ■ Verrouiller l'ordinateur ■ Présenter la boîte de dialogue PIN ■ Aucune action
Autoriser le déblocage de la carte à puce	Détermine si la clé cryptographique peut être débloquée lors de la connexion.

Paramètre de stratégie	Explication
OPTIONS DE VERROUILLAGE	
Verrouiller l'écran après X minutes d'inactivité	Détermine le délai à l'issue duquel un bureau inutilisé est automatiquement verrouillé. La valeur par défaut est de 0 minute, auquel cas le bureau n'est pas verrouillé.
Verrouiller l'écran au retrait de la carte à puce	Détermine si l'écran est verrouillé lorsqu'une clé cryptographique est retirée au cours d'une session.
Verrouiller l'écran après mise en veille	Détermine si l'écran est verrouillé si l'ordinateur est réactivé du mode veille.

15.3 Création d'une liste de codes PIN interdits à utiliser dans les stratégies

Pour les stratégies de type **PIN**, une liste de codes PIN interdits peut être créée afin de définir quelles sont les séquences de caractères qui ne doivent pas être utilisées dans les codes PIN.

Remarque: Dans les listes, les codes PIN non autorisés sont séparés par un espace ou un saut de ligne.

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans SafeGuard Management Center. La taille maximale de ces fichiers texte est de **50 Ko**. SafeGuard Enterprise n'utilise que des textes codés en Unicode UTF-16. Si vous ne créez pas les fichiers texte dans ce format, ils sont convertis automatiquement lors de l'enregistrement.

Si une conversion s'impose, un message s'affiche et indique que le fichier est en cours de conversion.

Pour enregistrer des fichiers texte, procédez comme suit :

1. Dans la zone de navigation de stratégie, cliquez avec le bouton droit de la souris sur **Texte d'informations** et sélectionnez **Nouveau > Texte**.
2. Entrez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.
3. Cliquez sur **[...]** pour sélectionner le fichier texte préalablement créé. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Texte d'informations** dans la zone de navigation de stratégie. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

Remarque: Grâce au bouton **Modifier le texte**, vous pouvez ajouter du texte au texte existant. Une boîte de dialogue de sélection d'un autre fichier texte s'affiche lorsque vous cliquez sur ce bouton. Le texte contenu dans ce fichier est ajouté à la fin du texte existant.

15.4 Règles de syntaxe des codes PIN

Les codes PIN peuvent comporter des nombres, des lettres et des caractères spéciaux (par exemple + - ; etc.). Toutefois, lorsque vous générez un nouveau code PIN, n'utilisez pas de caractère avec la combinaison ALT + < caractère > car ce mode de saisie n'est pas disponible lors de l'authentification au démarrage (POA). Les règles relatives aux codes PIN utilisés pour se connecter au système sont définies dans des stratégies du type **PIN**.

Avis : si des règles de mot de passe ont été définies dans SafeGuard Management Center, aucune règle ne doit être définie dans Active Directory.

Paramètre de stratégie	Explication
RÈGLES	
Longueur min. PIN	Affiche le nombre de caractères que doit contenir un code PIN lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Longueur max. PIN	Affiche le nombre maximum de caractères que doit contenir un code PIN lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Nombre min. de lettres Nombre min. de chiffres Nombre min. de caractères spéciaux	Ce paramètre spécifie qu'un code PIN ne peut pas contenir seulement des lettres, des nombres ou des caractères spéciaux mais doit comporter une combinaison de ces 2 au moins (par ex. 15fleur, etc.). Ce paramètre n'est pratique que si vous avez défini une longueur minimum de code PIN supérieure à 2.
Respecter la casse	Ce paramètre ne s'applique qu'avec **Utiliser la liste des codes PIN interdits** et **Utilisation interdite du nom d'utilisateur en tant que code PIN**. **Cas 1 :** vous avez saisi « tableau » dans la liste des codes PIN interdits. Si l'option **Respecter la casse** est définie sur OUI, les variantes supplémentaires du mot de passe telles que TABLEAU, TablEAU ne seront pas acceptées et la connexion sera refusée. **Cas 2 :** « EMaier » est saisi comme nom d'utilisateur. Si l'option **Respecter la casse** est définie sur OUI et que l'option **Utilisation interdite du nom d'utilisateur en tant que code PIN** est définie sur NON, l'utilisateur EMaier ne peut utiliser aucune variante de ce nom d'utilisateur (par ex. « emaier » ou « eMaiER ») comme code PIN.

Paramètre de stratégie	Explication
Interdire la succession de touches horizontales	Les séquences de touches consécutives sont, par exemple « 123 » ou « aze ». Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire la succession de touches verticales	Concerne les touches disposées consécutivement en colonne sur le clavier, par exemple « wqa1 », « xsz2 » ou « 3edc » (mais pas « wse4 », « xdr5 » ou « cft6 »). Un maximum de deux symboles adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme codes PIN. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Au moins 3 caractères consécutifs non autorisés	L'activation de cette option interdit les séquences de touches ■ qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant (« abc » ; « cba » ; « ;< », etc.) ; ■ constituées de trois symboles identiques ou plus (« aaa » ou « 111 »).
Utilisation interdite du nom d'utilisateur en tant que code PIN	Détermine si le nom d'utilisateur et le code PIN peuvent être identiques. **OUI :** l'utilisateur peut utiliser son nom d'utilisateur Windows comme code PIN. **NON :** le nom d'utilisateur Windows et le code PIN doivent être différents.
Utiliser la liste de PIN non autorisés	Détermine si certaines séquences de caractères ne doivent pas être utilisées pour les codes PIN. Les séquences de caractères sont stockées dans la liste des codes PIN non autorisés (par ex. fichier .txt).

Paramètre de stratégie	Explication
Liste de PIN non autorisés	Définit les séquences de caractères à ne pas utiliser pour les codes PIN. Si un utilisateur utilise un code PIN non autorisé, un message d'erreur s'affiche. **Conditions préalables importantes :** Une liste (fichier) de code PIN non autorisés doit être enregistrée dans Management Center, dans la zone de navigation de stratégie sous **Texte d'informations**. La liste n'est disponible qu'après l'enregistrement. Taille de fichier maximale : 50 Ko Format pris en charge : Unicode **Définition des codes PIN interdits** Dans la liste, les codes PIN non autorisés sont séparés par un espace ou un saut de ligne. *Le caractère générique* : Le caractère générique « * » peut représenter tout caractère et tout nombre de caractères dans un code PIN. Par exemple, *123* signifie que toute séquence de caractères contenant 123 sera interdite comme code PIN. **Avis :** ■ Si la liste ne contient qu'un seul caractère générique, l'utilisateur ne sera plus en mesure de se connecter au système après un changement obligatoire de mot de passe. ■ Les utilisateurs ne doivent pas être autorisés à accéder à ce fichier. ■ L'option **Utiliser la liste des codes PIN interdits** doit être activée.
MODIFICATIONS	
Modification du PIN après (jours) min.	Détermine la période pendant laquelle un mot de passe ne peut être modifié. Ce paramètre empêche l'utilisateur de changer un mot de passe trop souvent au cours d'une période donnée. **Exemple :** l'utilisateur Miller définit un nouveau code PIN (par ex. « 13jk56 »). L'intervalle minimum de changement pour cet utilisateur (ou pour le groupe auquel il appartient) est défini à cinq jours. Après deux jours seulement, l'utilisateur décide de remplacer le code PIN par « 13jk56 ». Le changement de code PIN est refusé car Mme Miller ne peut définir un nouveau mot de passe qu'après un délai de cinq jours.

Paramètre de stratégie	Explication
Modification du PIN après (jours) max.	Si la période de validité maximum est activée, l'utilisateur doit définir un nouveau code PIN une fois la période définie expirée.
Notifier une modification forcée avant (jours)	Un message d'avertissement s'affiche « n » jours avant l'expiration du code PIN pour rappeler à l'utilisateur de changer son code PIN dans « n » jours. L'utilisateur peut également le changer immédiatement.
GÉNÉRAL	
Longueur d'historique PIN	Détermine à quel moment des codes PIN déjà utilisés peuvent l'être à nouveau. Il convient de définir la longueur d'historique avec le paramètre **Modification du PIN après (jours) max.**. **Exemple :** La longueur d'historique du code PIN pour l'utilisateur Miller est définie à 4 et le nombre de jours à l'issue desquels l'utilisateur doit changer son code PIN est de 30. M. Miller se connecte actuellement en utilisant le code PIN « Informatik ». Lorsque la période de 30 jours expire, il est invité à changer son code PIN. M. Miller saisit « Informatik » comme nouveau code PIN et reçoit un message d'erreur indiquant que ce code PIN a déjà été utilisé et qu'il doit en sélectionner un nouveau. M. Miller ne peut pas utiliser le code PIN « Informatik » avant la quatrième invitation de changement du code PIN (en d'autres termes, longueur d'historique du code PIN = 4).

15.5 Création d'une liste de mots de passe interdits à utiliser dans les stratégies

Pour les stratégies de type **Mot de passe** une liste de mots de passe peut être créée afin de définir quelles sont les séquences de caractères qui ne doivent pas être utilisées dans les mots de passe :

Remarque: Dans les listes, les mots de passe non autorisés sont séparés par un saut de ligne.

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans SafeGuard Management Center. La taille maximale de ces fichiers texte est de **50 Ko**. SafeGuard Enterprise n'utilise que des textes codés en Unicode UTF-16. Si vous ne créez pas les fichiers texte dans ce format, ils sont convertis automatiquement lors de l'enregistrement.

Si une conversion s'impose, un message s'affiche et indique que le fichier est en cours de conversion.

Pour enregistrer des fichiers texte, procédez comme suit :

1. Dans la zone de navigation de stratégie, cliquez avec le bouton droit de la souris sur **Texte d'informations** et sélectionnez **Nouveau > Texte**.
2. Entrez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.
3. Cliquez sur **[...]** pour sélectionner le fichier texte préalablement créé. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Texte d'informations** dans la zone de navigation de stratégie. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

Remarque: Grâce au bouton **Modifier le texte**, vous pouvez ajouter du texte au texte existant. Une boîte de dialogue de sélection d'un autre fichier texte s'affiche lorsque vous cliquez sur ce bouton. Le texte contenu dans ce fichier est ajouté à la fin du texte existant.

15.6 Règles de syntaxe des mots de passe

Les mots de passe peuvent comporter des nombres, des lettres et des caractères spéciaux (par exemple + - ; etc.). Toutefois, lorsque vous générez un nouveau mot de passe, n'utilisez pas de caractère avec la combinaison ALT + < caractère > car ce mode de saisie n'est pas disponible lors de l'authentification au démarrage (POA). Les règles relatives aux mots de passe utilisés pour se connecter au système sont définies dans des stratégies du type **Mot de passe**.

Avis : si des règles de mot de passe ont été définies dans SafeGuard Enterprise Management Center, aucune règle ne doit être définie dans Active Directory.

Paramètre de stratégie	Explication
RÈGLES	
Longueur min. mot de passe	Affiche le nombre de caractères que doit contenir un mot de passe lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Longueur max. mot de passe	Affiche le nombre maximum de caractères que doit contenir un mot de passe lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Nombre min. de lettres Nombre min. de chiffres Nombre min. de caractères spéciaux	Ce paramètre spécifie qu'un mot de passe ne peut pas contenir seulement des lettres, des nombres ou des caractères spéciaux mais doit comporter une combinaison de ces 2 au moins (par ex. 15fleur, etc.). Ce paramètre n'est pratique que si vous avez défini une longueur minimum de mot de passe supérieure à 2.
Respecter la casse	Ce paramètre ne s'applique qu'avec **Utiliser la liste des mots de passe interdits** et **Utilisation interdite du nom d'utilisateur en tant que mot de passe**. **Cas 1 :** vous avez saisi « tableau » dans la liste des mots de passe interdits. Si l'option **Respecter la casse** est définie sur OUI, les variantes supplémentaires du mot de passe telles que TABLEAU, TablEAU ne seront pas acceptées et la connexion sera refusée. **Cas 2 :** « EMaier » est saisi comme nom d'utilisateur. Si l'option **Respecter la casse** est définie sur OUI et que l'option **Utilisation interdite du nom d'utilisateur en tant que mot de passe** est définie sur NON, l'utilisateur EMaier ne peut utiliser aucune variante de ce nom d'utilisateur (par ex. « emaier » ou « eMaiER ») comme mot de passe.

Paramètre de stratégie	Explication
Interdire la succession de touches horizontales	Les séquences de touches consécutives sont, par exemple « 123 » ou « aze ». Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire la succession de touches verticales	Concerne les touches disposées consécutivement en colonne sur le clavier, par exemple « wqa1 », « xsz2 » ou « 3edc » (mais pas « wse4 », « xdr5 » ou « cft6 »). Un maximum de deux symboles adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme mot de passe. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Au moins 3 caractères consécutifs non autorisés	L'activation de cette option interdit les séquences de touches ■ qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant (« abc » ; « cba » ; « ;< », etc.) ; ■ constituées de trois symboles identiques ou plus (« aaa » ou « 111 »).
Nom d'utilisateur comme mot de passe non autorisé	Détermine si le nom d'utilisateur et le mot de passe peuvent être identiques. **OUI :** le nom d'utilisateur Windows et le mot de passe doivent être différents. **NON :** l'utilisateur peut utiliser son nom d'utilisateur Windows comme mot de passe.
Utiliser la liste de mots de passe non autorisés	Détermine si certaines séquences de caractères ne doivent pas être utilisées pour les mots de passe. Les séquences de caractères sont stockées dans la liste des mots de passe interdits (par ex. fichier .txt).

Paramètre de stratégie	Explication
Liste de mots de passe non autorisés	Définit les séquences de caractères à ne pas utiliser pour les mots de passe. Si un utilisateur utilise un mot de passe non autorisé, un message d'erreur s'affiche. **Conditions préalables importantes :** Une liste (fichier) de mots de passe non autorisés doit être enregistrée dans Management Center, dans la zone de navigation de stratégie sous **Texte d'informations**. La liste n'est disponible qu'après l'enregistrement. Taille de fichier maximale : 50 Ko Format pris en charge : Unicode **Définition de mots de passe interdits** Dans la liste, les mots de passe non autorisés sont séparés par un saut de ligne. *Le caractère générique* : le caractère générique « * » peut représenter tout caractère et tout nombre de caractères dans un mot de passe. Par exemple, *123* signifie que toute séquence de caractères contenant 123 sera interdite comme mot de passe. Avis : ■ Si la liste ne contient qu'un seul caractère générique, l'utilisateur ne sera plus en mesure de se connecter au système après un changement obligatoire de mot de passe. ■ Les utilisateurs ne doivent pas être autorisés à accéder à ce fichier. ■ L'option **Utiliser la liste des mots de passe interdits** doit être activée.

Paramètre de stratégie	Explication
Synchronisation du mot de passe de l'utilisateur avec les autres clients SGN	Ce champ détermine la procédure de synchronisation des mots de passe lorsque des utilisateurs utilisant plusieurs PC utilisateur SafeGuard Enterprise, et définis comme les utilisateurs de ces ordinateurs, changent leurs mots de passe. Les options suivantes sont disponibles : ■ Lent (attendre que l'utilisateur se connecte) Si un utilisateur change son mot de passe sur un ordinateur final SafeGuard Enterprise et qu'il compte se connecter à un autre ordinateur sur lequel il est également enregistré, il doit tout d'abord se connecter avec son ancien mot de passe à l'authentification au démarrage. La synchronisation du mot de passe n'est effectuée qu'après la connexion avec l'ancien mot de passe. ■ Rapide (attendre la connexion de la machine) Si un utilisateur change son mot de passe sur un ordinateur final SafeGuard Enterprise, la synchronisation du mot de passe avec d'autres ordinateurs, sur lesquels l'utilisateur est également enregistré, est effectuée dès que l'autre ordinateur a établi une connexion avec le serveur. C'est le cas, par exemple, lorsqu'un autre utilisateur, également enregistré en tant qu'utilisateur de l'ordinateur, se connecte simultanément à l'ordinateur.
MODIFICATIONS	
Modification du mot de passe autorisée après (jours) min.	Détermine la période pendant laquelle un mot de passe ne peut être modifié. Ce paramètre empêche l'utilisateur de changer un mot de passe trop souvent au cours d'une période donnée. Si l'utilisateur est forcé à changer son mot de passe par Windows ou s'il modifie son mot de passe après l'affichage du message d'avertissement indiquant que le mot de passe expirera dans X jours, ce paramètre ne sera pas évalué. **Exemple :** l'utilisateur Miller définit un nouveau mot de passe (par ex. « 13jk56 »). L'intervalle minimum de changement pour cet utilisateur (ou pour le groupe auquel il appartient) est défini à cinq jours. Après deux jours seulement, l'utilisateur décide de changer le mot de passe par « 13jk56 ». Le changement de mot de passe est refusé car Mme Miller ne peut définir un nouveau mot de passe qu'après un délai de cinq jours.

Paramètre de stratégie	Explication
Le mot de passe expire dans (jours)	Si la période de validité maximum est activée, l'utilisateur doit définir un nouveau mot de passe une fois la période définie expirée.
Notifier une modification forcée avant (jours)	Un message d'avertissement s'affiche « n » jours avant l'expiration du mot de passe pour rappeler à l'utilisateur de changer son mot de passe dans « n » jours. L'utilisateur peut également le changer immédiatement.
GÉNÉRAL	
Longueur de l'historique du mot de passe	Détermine à quel moment des mots de passe déjà utilisés peuvent l'être à nouveau. Il convient de définir la longueur d'historique avec le paramètre « Expiration du mot de passe après (jours) ». **Exemple :** La longueur d'historique du mot de passe pour l'utilisateur Miller est définie à 4 et le nombre de jours à l'issue desquels l'utilisateur doit changer son mot de passe est de 30. M. Miller se connecte actuellement en utilisant le mot de passe « Informatik ». Lorsque la période de 30 jours expire, il est invité à changer son mot de passe. M. Miller saisit « Informatik » comme nouveau mot de passe et reçoit un message d'erreur indiquant que ce mot de passe est déjà utilisé et qu'il doit en sélectionner un nouveau. M. Miller ne peut pas utiliser le mot de passe « Informatik » avant la quatrième invitation de changement du mot de passe (en d'autres termes, longueur d'historique du mot de passe = 4).

15.7 Passphrase pour SafeGuard Data Exchange

L'utilisateur doit saisir une passphrase pour l'échange de données sécurisé via SafeGuard Data Exchange qui est utilisé pour générer des clés locales. Les clés générées sur les ordinateurs finaux sont également stockées dans la base de données SafeGuard Enterprise. La configuration minimale est définie dans les stratégies du type **Passphrase**.
Pour plus d'informations sur SafeGuard Data Exchange et sur SafeGuard Portable, consultez l'aide de l'utilisateur de SafeGuard Enterprise.

Paramètre de stratégie	Explication
RÈGLES	
Longueur min. passphrase	Définit le nombre minimum de caractères de la passphrase à partir de laquelle la clé est générée. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Longueur max. passphrase	Définit le nombre maximum de caractères de la passphrase. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Nombre min. de lettres Nombre min. de chiffres Nombre min. de caractères spéciaux	Ce paramètre spécifie qu'une passphrase ne peut pas contenir seulement des lettres, des nombres ou des symboles mais doit comporter une combinaison de ces 2 au moins (par ex. 15 fleur etc.). Ce paramètre n'est pratique que si vous avez défini une longueur minimum de passphrase supérieure à 2.
Respecter la casse	Ce paramètre est effectif lorsque l'option « **Utilisation interdite du nom d'utilisateur en tant que passphrase** » est active. **Exemple :** « EMaier » est saisi comme nom d'utilisateur. Si l'option **Respecter la casse** est définie sur OUI et si **Utilisation interdite du nom d'utilisateur en tant que passphrase** est définie sur NON, l'utilisateur EMaier ne peut utiliser aucune variante de ce nom d'utilisateur (par exemple emaier ou eMaiER) comme passphrase.
Interdire la succession de touches horizontales	Les séquences de touches consécutives sont, par exemple « 123 » ou « aze ». Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.

Paramètre de stratégie	Explication
Interdire la succession de touches verticales	Concerne les touches disposées consécutivement en colonne sur le clavier, par exemple « wqa1 », « xsz2 » ou « 3edc » (mais pas « wse4 », « xdr5 » ou « cft6 »). Un maximum de deux caractères adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme mots de passe. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Au moins 3 caractères consécutifs non autorisés	L'activation de cette option interdit les séquences de touches ■ qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant (« abc » ; « cba » ; « ;< », etc.) ; ■ constituées de trois symboles identiques ou plus (« aaa » ou « 111 »).
Utilisation interdite du nom d'utilisateur en tant que passphrase	Détermine si le nom d'utilisateur et la passphrase peuvent être identiques. **OUI :** le nom d'utilisateur Windows et la passphrase doivent être différents. **NON :** l'utilisateur peut utiliser son nom d'utilisateur Windows comme passphrase.

15.8 Protection du périphérique

La fonction principale de SafeGuard Enterprise est le chiffrement des données sur des périphériques de stockage de données différents. Le chiffrement peut être basé sur volume ou sur fichier avec des clés et des algorithmes différents. Les stratégies du type **Protection du périphérique** incluent également des paramètres pour SafeGuard Data Exchange et SafeGuard Portable. Pour plus d'informations sur SafeGuard Data Exchange et SafeGuard Portable, consultez l'aide de l'utilisateur de SafeGuard Enterprise.

Paramètre de stratégie	Explication
Mode de déchiffrement des supports	Permet de protéger les périphériques (PC, ordinateurs portatifs et assistants numériques personnels) ainsi que tous types de supports amovibles. L'objectif essentiel consiste à chiffrer toutes les données stockées sur des périphériques de stockage locaux ou externes. Cette méthode transparente permet aux utilisateurs de continuer à utiliser leurs applications courantes, par exemple Microsoft Office. Le chiffrement transparent signifie que toutes les données chiffrées (dans des répertoires ou dans des volumes chiffrés) sont automatiquement déchiffrées dans la mémoire principale dès qu'elles sont ouvertes dans un programme. Un fichier est automatiquement chiffré de nouveau lorsqu'il est enregistré. Les options suivantes sont disponibles : ■ **Aucun chiffrement** ■ **Basé sur volume (= chiffrement transparent basé sur secteur)** Garantit que toutes les données sont chiffrées (y compris les fichiers d'initialisation, les fichiers d'échange, les fichiers inactifs/d'hibernation, les fichiers temporaires, les informations de répertoire, etc.) sans que l'utilisateur doive modifier ses habitudes de travail ou tenir compte de problèmes de sécurité. **Avis :** Si une stratégie de chiffrement existe pour un volume ou un type de volume et que le chiffrement de ce dernier échoue, l'utilisateur n'est pas autorisé à y accéder.

Paramètre de stratégie	Explication
	Partition système Windows 7 : Sachez que pour Windows 7 Professionnel, Entreprise et Édition intégrale, une partition système est créée sur les ordinateurs finaux sans attribution de lettre de lecteur. Cette partition système ne peut pas être chiffrée par SafeGuard Enterprise. **Accès à des objets de système de fichiers non identifiés** : Les objets de système de fichiers non identifiés sont des volumes pour lesquels SafeGuard Enterprise ne peut pas clairement définir s'ils sont bruts ou chiffrés par un périphérique. Si une stratégie de chiffrement existe pour un objet de système de fichiers non identifié, l'accès à ce volume est refusé. Si aucune stratégie de chiffrement n'existe, l'utilisateur peut accéder au volume. **Avis :** si une stratégie de chiffrement avec l'option **Clé à utiliser pour le chiffrement** définie pour activer la sélection de clé (par exemple **Toute clé du jeu de clés utilisateur**) existe pour un volume d'objet de système de fichiers non identifié, un certain temps s'écoule entre l'affichage de la boîte de dialogue de sélection de la clé et le refus de l'accès. Pendant ce laps de temps, le volume est accessible. Tant que la boîte de dialogue de sélection de clé n'est pas confirmée, le volume est accessible. Pour éviter cela, indiquez une clé présélectionnée pour le chiffrement (voir la description du paramètre de stratégie **Clé à utiliser pour le chiffrement**). De plus, ce laps de temps se produit également pour les volumes d'objets de système de fichiers non identifiés connectés à un ordinateur final si l'utilisateur a déjà ouvert des fichiers sur le volume au moment où une stratégie de chiffrement prend effet. Dans ce cas, il ne peut être garanti que l'accès au volume sera refusé, car cela pourrait entraîner une perte de données. **Volumes pour lesquels la fonction d'exécution automatique est activée :** Si l'exécution automatique est activée pour un volume pour lequel une stratégie de chiffrement existe, les problèmes suivants ont lieu : ■ Le volume n'est pas chiffré. ■ Si le volume est un objet de fichier non identifié, l'accès n'est pas refusé.

Paramètre de stratégie	Explication
	Accès aux volumes chiffrés par BitLocker To Go : Si SafeGuard Enterprise est utilisé avec la prise en charge BitLocker To Go activée et qu'une stratégie de chiffrement SafeGuard Enterprise existe pour un volume chiffré BitLocker To Go, l'accès au volume est refusé. Si aucune stratégie de chiffrement SafeGuard Enterprise n'existe, l'utilisateur peut accéder au volume. **Avis :** si les paramètres d'exécution automatique d'une clé USB chiffrée par BitLocker To Go sont définis sur les valeurs par défaut, il se peut que l'accès ne soit pas refusé malgré la stratégie de chiffrement SafeGuard Enterprise. Ceci ne se produit que sous Windows Vista. ■ Pour plus d'informations sur BitLocker To Go, voir *SafeGuard Enterprise et BitLocker To Go* en page 296 ■ **Basé sur fichier** (= chiffrement transparent basé sur fichier (Chiffrement Smart Media)) Garantit que toutes les données sont chiffrées (à l'exception du support d'initialisation et des informations de répertoire) avec l'avantage que même les supports optiques tels que les CD/DVD peuvent être chiffrés et que les données peuvent être échangées avec des ordinateurs externes sur lesquels SafeGuard n'est pas installé (si les stratégies l'autorisent). **Avis :** les données chiffrées à l'aide de la méthode « Chiffrement basé sur fichier » ne peuvent pas être compressées. De même, les données compressées ne peuvent pas être chiffrées en utilisant le chiffrement basé sur fichier. Les volumes d'initialisation ne sont jamais chiffrés selon la méthode basée sur fichier. Ils sont automatiquement exclus du chiffrement basé sur fichier, même si une règle correspondante est définie.
PARAMÈTRES GÉNÉRAUX	
Algorithme à utiliser pour le chiffrement	Définit l'algorithme de chiffrement. Liste des algorithmes utilisables avec les normes respectives : AES256 : 32 octets (256 bits) AES128 : 16 octets (128 bits) AES256 avec diffuseur AES128 avec diffuseur

Paramètre de stratégie	Explication
Clé à utiliser pour le chiffrement	Définit la clé utilisée pour le chiffrement. Vous pouvez définir des clés spécifiques (clé machine ou une clé définie par ex.) ou vous pouvez autoriser l'utilisateur à sélectionner une clé. Vous pouvez également limiter les clés qu'un utilisateur est autorisé à utiliser. Les options suivantes sont disponibles : ■ **Toute clé du jeu de clés utilisateur** Toutes les clés d'un jeu de clés utilisateur sont affichées et celui-ci peut sélectionner l'une d'entre elles. **Avis :** cette option doit être sélectionnée si vous définissez une stratégie de chiffrement basé sur fichier pour un ordinateur final non géré protégé par SafeGuard Enterprise (autonome). ■ **Toute clé du jeu de clés utilisateur** Toutes les clés sauf celles du jeu de clés d'un utilisateur sont affichées et celui-ci peut sélectionner l'une d'entre elles. ■ **Toute clé de groupe du jeu de clés utilisateur** Toutes les clés de groupe du jeu de clés d'un utilisateur sont affichées et celui-ci peut sélectionner l'une d'entre elles. ■ **Clé machine définie :** La clé de la machine est utilisée, l'utilisateur ne peut PAS sélectionner de clé. **Avis :** cette option doit être sélectionnée si vous définissez une stratégie de chiffrement basé sur volume pour un ordinateur final non géré protégé par SafeGuard Enterprise (mode autonome). Si vous sélectionnez néanmoins **Toute clé du jeu de clés utilisateur** et que l'utilisateur sélectionne une clé créée localement pour le chiffrement basé sur volume, l'accès à ce volume sera refusé. ■ **Toute clé du jeu de clés utilisateur sauf les clés créées localement** Toutes les clés sauf les clés générées localement à partir d'un jeu de clés sont affichées et l'utilisateur peut sélectionner l'une d'entre elles. ■ **Clé définie dans la liste** L'administrateur peut sélectionner n'importe quelle clé disponible lorsqu'il définit des stratégies dans Management Center.

Paramètre de stratégie	Explication
	La clé doit être sélectionnée sous **Clé définie pour le chiffrement**. **Avis :** **Si l'option Clé machine définie est utilisée** Si SafeGuard Enterprise Device Encryption n'est pas installé sur un ordinateur final (pas de POA, pas de chiffrement basé sur volume), une stratégie définissant la **Clé machine définie** comme étant la clé à utiliser pour le chiffrement basé sur fichier ne s'appliquera pas sur cet ordinateur. La clé machine définie n'est pas disponible sur un ordinateur de ce type. Les données ne peuvent pas être chiffrées. **Stratégies pour les ordinateurs finaux non gérés protégés par SafeGuard Enterprise (autonome) :** Notez que seule l'option **Toute clé du jeu de clés utilisateur** peut être utilisée lors de la création de stratégies pour des ordinateurs finaux non gérés. La création de clés locales doit en outre être autorisée pour ce type d'ordinateur final. Si la fonction de passphrase de support est activée pour des ordinateurs finaux non gérés, la clé de chiffrement de support est utilisée automatiquement comme **Clé définie pour le chiffrement** car aucune clé de groupe n'est disponible sur les ordinateurs finaux non gérés. La sélection d'une autre clé sous Clé définie pour le chiffrement lors de la création d'une stratégie de support amovible pour des ordinateurs finaux non gérés n'a aucun effet.

Paramètre de stratégie	Explication
Clé définie pour le chiffrement	Ce champ ne devient actif que si vous avez sélectionné l'option **Clé définie dans la liste** dans le champ **Clé à utiliser pour le chiffrement**. Cliquez sur [**...**] pour afficher la boîte de dialogue **Rechercher des clés**. Cliquez sur **Rechercher maintenant** pour rechercher des clés et en sélectionner une dans la liste qui apparaît. Pour une stratégie du type Protection du périphérique avec une cible : Supports amovibles, cette clé est utilisée pour chiffrer la clé de chiffrement de support lorsque la fonction de passphrase de support est activée (l'utilisateur peut définir une passphrase pour un périphérique : Oui) Pour des stratégies Protection du périphérique pour des supports amovibles, les paramètres ■ Clé à utiliser pour le chiffrement ■ Clé définie pour le chiffrement doivent être spécifiés séparément. **Stratégies pour les ordinateurs finaux non gérés protégés par SafeGuard Enterprise (autonome) :** Si la fonction de passphrase de support est activée pour des ordinateurs finaux non gérés, la clé de chiffrement de support est utilisée automatiquement comme **Clé définie pour le chiffrement** car aucune clé de groupe n'est disponible sur les ordinateurs finaux non gérés.
L'utilisateur est autorisé à créer une clé locale	Ce paramètre détermine si l'utilisateur peut générer ou non une clé locale sur son ordinateur. Les clés locales sont générées sur l'ordinateur final selon un mot de passe saisi par l'utilisateur. La configuration minimale du mot de passe est définie dans les stratégies du type **Passphrase**. Ces clés sont également enregistrées dans la base de données. L'utilisateur peut les utiliser sur n'importe quel ordinateur auquel il est connecté. Des clés locales peuvent être utilisées pour l'échange de données sécurisé via SafeGuard Data Exchange (SG DX).

Paramètre de stratégie	Explication
PARAMÈTRES BASÉS SUR VOLUME	
L'utilisateur peut ajouter des clés au volume chiffré ou les en supprimer	**OUI :** les utilisateurs de l'ordinateur final peuvent ajouter ou supprimer des clés d'un jeu de clés. La boîte de dialogue s'affiche via la commande du menu contextuel **Chiffrement** / onglet **Chiffrement**. **NON :** les utilisateurs de l'ordinateur final ne peuvent pas ajouter de clés.
Réaction aux volumes non chiffrés	Définit de quelle manière SafeGuard Enterprise gère les supports non chiffrés : Les options suivantes sont disponibles : ■ Rejeter (= le support en texte n'est pas chiffré) ■ N'accepter que les supports vierges et chiffrer ■ Accepter tous les supports et chiffrer
L'utilisateur peut déchiffrer un volume	Permet à l'utilisateur de déchiffrer le volume par l'intermédiaire d'une commande du menu contextuel dans l'Explorateur Windows.
Chiffrement initial rapide	Sélectionnez ce paramètre pour activer le mode de chiffrement initial rapide pour le chiffrement basé sur fichier. Ce mode permet de réduire la durée nécessaire au chiffrement initial sur des ordinateurs de points de terminaison. **Avis :** Ce mode peut se traduire par une sécurité inférieure.
Poursuivre sur les secteurs incorrects	Indique si le chiffrement doit se poursuivre ou être arrêté si des secteurs incorrects sont détectés. Le paramètre par défaut est OUI.
PARAMÈTRES BASÉS SUR FICHIER	
Chiffrement initial de tous les fichiers	Démarre automatiquement le chiffrement initial d'un volume après la connexion de l'utilisateur. Il se peut que l'utilisateur doive sélectionner une clé du jeu de clé au préalable.
L'utilisateur peut annuler le chiffrement initial	Permet à l'utilisateur d'annuler le chiffrement initial.
L'utilisateur n'est pas autorisé à accéder aux fichiers non chiffrés	Définit si un utilisateur peut accéder aux données non chiffrées d'un volume.

Paramètre de stratégie	Explication
L'utilisateur peut déchiffrer des fichiers	Permet à un utilisateur de déchiffrer des fichiers individuels ou des répertoires entiers (en utilisant l'extension de l'Explorateur Windows <clic droit>).
L'utilisateur peut définir une passphrase (de support) pour les périphériques	Permet à l'utilisateur de définir une passphrase de support sur son ordinateur. La passphrase de support permet d'accéder facilement via SafeGuard Portable à toutes les clés locales utilisées sur des ordinateurs sur lesquels SafeGuard Data Exchange n'est pas installé.
Applications non gérées	Permet de définir d'autres applications devant être ignorées par le pilote du filtre SafeGuard Enterprise et devant être exclues du chiffrement/déchiffrement transparent. Le séparateur à utiliser pour ces applications est « ; ». Un exemple d'application non gérée est un programme de sauvegarde. Pour garantir que ces données ne sont pas déchiffrées lors de la création d'une sauvegarde, cette application peut être exclue du processus de chiffrement/déchiffrement. Les données sont sauvegardées sous forme chiffrée. **Avis :** comme il s'agit de paramètres spécifiques de la machine, ils ne sont appliqués que lorsque l'ordinateur final est réinitialisé. **Définition des applications non gérées** Utilisation générale : Les programmes de sauvegarde peuvent être définis comme exemptés afin qu'ils puissent toujours lire et enregistrer les données chiffrées. Les applications susceptibles de déclencher des dysfonctionnements lorsqu'elles sont utilisées avec SafeGuard Enterprise mais qui ne nécessitent pas de chiffrement peuvent généralement être exemptées de chiffrement. Le nom complet du fichier exécutable (contenant éventuellement les informations du chemin d'accès) est utilisé pour spécifier une application exemptée. **Avis :** des applications non gérées ne peuvent être définies que pour des **périphériques de stockage locaux**. Pour une stratégie globale du type **Protection du périphérique**, la cible **Périphériques de stockage locaux** doit être sélectionnée. Pour toutes les autres cibles, l'option **Applications non gérées** n'est pas disponible.

Paramètre de stratégie	Explication
Supports amovibles seulement Copier portable SG vers support amovible	Si cette option est activée, SafeGuard Portable est copié sur tout support amovible connecté à l'ordinateur final. SafeGuard Portable permet l'échange des données chiffrées avec le support amovible sans que SafeGuard Enterprise ne soit installé sur le destinataire. Le destinataire peut déchiffrer et rechiffrer les fichiers chiffrés en utilisant SafeGuard Portable et le mot de passe correspondant. Le destinataire peut rechiffrer les fichiers avec SafeGuard Portable ou utiliser la clé d'origine pour le chiffrement. Il n'est pas nécessaire que SafeGuard Portable soit installé ou copié sur l'ordinateur du destinataire, il peut être utilisé directement à partir du support amovible.
Clé de chiffrement initial par défaut	Ce champ propose une boîte de dialogue de sélection d'une clé utilisée pour le chiffrement initial basé sur fichier. Si vous sélectionnez une clé ici, l'utilisateur ne peut pas sélectionner de clé au démarrage du chiffrement initial. Le chiffrement initial démarre sans interaction de l'utilisateur. La clé sélectionnée est toujours utilisée pour le chiffrement initial. **Exemple :** Condition préalable : Une clé par défaut a été définie pour le chiffrement initial. Le chiffrement initial démarre automatiquement lorsque l'utilisateur connecte un périphérique USB à l'ordinateur. La clé définie est utilisée. L'utilisateur ne doit pas intervenir. Si l'utilisateur souhaite rechiffrer les fichiers ou enregistrer de nouveaux fichiers sur le périphérique USB, il peut sélectionner une quelconque clé (s'il y est autorisé et si disponible). Si l'utilisateur connecte un autre périphérique USB, la clé définie pour le chiffrement initial est de nouveau utilisée. Cette clé est également utilisée pour tous les processus de chiffrement ultérieurs jusqu'à ce que l'utilisateur sélectionne explicitement une autre clé. **Avis :** cette option est désactivée lorsque la fonction de passphrase de support est activée. La **Clé définie pour le chiffrement** sera utilisée.
Dossier en texte brut	Le dossier spécifié ici sera créé sur chaque support amovible. Les fichiers copiés dans ce dossier restent au format brut.

15.9 Paramètres spécifiques de la machine – Paramètres de base

Paramètre de stratégie	Explication
AUTHENTIFICATION AU DÉMARRAGE (POA)	
Activer l'authentification au démarrage	Définit si l'authentification au démarrage est activée ou désactivée en permanence. **Avis :** pour des raisons de sécurité, il est fortement recommandé que l'authentification au démarrage reste activée. La désactivation de l'authentification au démarrage réduit la sécurité système à la sécurité à l'ouverture de session Windows et augmente le risque d'accès non autorisé à des données chiffrées.
Interdire l'utilisateur invité	Définit si un utilisateur est autorisé à se connecter à Windows.
Accès refusé si aucune connexion au serveur pendant (jours) (0 =pas de contrôle)	Refuse la connexion dans POA si le PC n'a pas été connecté au serveur pendant une période supérieure à la période définie.
Seul l'utilisateur attribué peut se connecter	Définit si l'utilisateur est autorisé à se connecter à Windows. **OUI :** seul les utilisateurs reconnus dans POA peuvent se connecter. **NON :** les utilisateurs non reconnus dans POA peuvent se connecter.
Importation de nouveaux utilisateurs autorisée pour	Détermine si un autre utilisateur peut être ajouté à POA. Différencie les propriétaires de machines des autres utilisateurs présents dans POA.

Paramètre de stratégie	Explication
Éveil par appel réseau sécurisé (WOL)	La stratégie « Éveil par appel réseau sécurisé » permet à l'ordinateur final de se préparer aux déploiements de logiciels dans lesquels les paramètres nécessaires tels que la désactivation temporaire de POA et un intervalle d'éveil par appel réseau peuvent être importés directement dans l'ordinateur final et analysés par celui-ci. L'équipe de déploiement peut concevoir un script de programmation en utilisant les commandes fournies pour garantir la protection maximale de l'ordinateur final bien que POA soit désactivé. **N'oubliez pas que la désactivation du POA – même pour un nombre limité de processus d'initialisation – réduit le niveau de sécurité de votre système.** **EXEMPLE :** l'équipe de déploiement des logiciels notifie le SO de SafeGuard Enterprise concernant un déploiement planifié de logiciel prévu le 25 septembre 2008 entre 03 h 00 et 06 h 00 du matin. 2 réinitialisations sont requises. L'agent local de déploiement des logiciels doit être en mesure de se connecter à Windows. Le SO crée la stratégie suivante et l'attribue aux ordinateurs finaux correspondants : Nombre de connexions automatiques (0 = pas de WOL) : **5** Connexion à Windows autorisée pendant le WOL : **Oui** Début de la plage horaire pour le lancement du WOL externe : **24 Sept. 2009, 12 h 00** Fin de la plage horaire pour le lancement du WOL externe : **25 sept. 2009, 06:00** Le SO fournit un tampon de 3 pour les connexions automatiques.

Paramètre de stratégie	Explication
	Le responsable de la sécurité définit l'intervalle à 12 heures le jour précédant le déploiement pour permettre au script de programmation SGMCMDIntn.exe de démarrer rapidement et que l'éveil par appel réseau ne démarre pas après le 25 septembre à 3 heures du matin. L'équipe de déploiement des logiciels produit deux commandes pour le script de programmation : – démarrage 24 sept.2009, 12:15, SGMCMDIntn.exe / WOLstart – démarrage 26 sept.2009, 09:00 SGMCMDIntn.exe / WOLstop Le script de déploiement est daté du 25.09.2009, 03:00. L'éveil par appel réseau peut être à nouveau explicitement désactivé à la fin du script en utilisant SGMCMDIntn.exe / WOLstop. Tous les ordinateurs finaux qui se connectent avant le 24 septembre 2009 et qui se connectent aux serveurs de déploiement recevront la nouvelle stratégie et les commandes de programmation. Tout ordinateur final sur lequel la programmation déclenche la commande SGMCMDIntn/WOLstart entre le 24 sept. 2009 à midi et le 25 sept. 2009, à 6 heures du matin se trouve dans l'intervalle de l'éveil par appel réseau et ce dernier sera par conséquent activé.
Nombre de connexions automatiques	Définit le nombre de réinitialisations lorsque l'authentification au démarrage est inactive pour l'éveil par appel réseau. Ce paramètre remplace temporairement le paramètre **Activer l'authentification au démarrage** jusqu'à ce que le nombre prédéfini de connexions automatiques soit atteint. L'authentification au démarrage est ensuite réactivée. Exemple : le nombre de connexions automatiques est défini sur 2, « Activer l'authentification au démarrage » est activé. Le PC s'initialise deux fois sans authentification au démarrage via POA. Pour le mode Éveil par appel réseau, nous recommandons de toujours autoriser **trois réinitialisations de plus que nécessaire** pour faire face aux problèmes imprévus.
Connexion à Windows autorisée pendant le WOL	Détermine si la connexion Windows est autorisée pendant l'éveil par appel réseau, par ex. pour une mise à jour de logiciel. Ce paramètre est interprété par POA.

Paramètre de stratégie	Explication
Début de la plage horaire pour le lancement du WOL externe Fin de la plage horaire pour le lancement du WOL externe	La date et l'heure peuvent être sélectionnées ou saisies pour le début et la fin de l'éveil par appel réseau (WOL). Format de date : *MM/JJ/AAAA* Format d'heure : *HH:MM* Les combinaisons suivantes de saisie sont possibles : ■ début et fin de l'éveil par appel réseau définis ; ■ fin de l'éveil par appel réseau définie, début ouvert ; ■ pas de saisie : aucun intervalle n'a été défini. En cas de déploiement planifié de logiciel, le SO doit définir la plage de l'éveil par appel réseau de sorte que le script de programmation puisse démarrer suffisamment tôt pour accorder aux ordinateurs finaux le temps suffisant pour l'initialisation. WOLstart (Début WOL) : Le point de départ de l'éveil par appel réseau dans le script de programmation doit se trouver dans l'intervalle défini dans la stratégie. Si aucun intervalle n'est défini, l'éveil par appel réseau n'est pas activé localement sur l'ordinateur final protégé par SafeGuard Enterprise. WOLstop (Fin WOL) : Cette commande s'effectue quel que soit le point final défini pour l'éveil par appel réseau. **Avis :** depuis la version 5.20, un paramètre d'éveil par appel réseau ne sera effectif que si un intervalle a été défini. Dans le cas d'une mise à jour de version, ceci signifie également que les stratégies d'éveil par appel réseau définies dans la version 5.10 ne seront plus effectives au départ. Après la migration, le responsable de la sécurité devra définir une plage pour ces stratégies en supplément.
OPTIONS D'AFFICHAGE	
Afficher l'identification de la machine	Affiche le nom de l'ordinateur ou un texte défini dans la barre de titre du POA. Si les paramètres réseau de Windows incluent le nom de la machine, ce dernier est automatiquement intégré aux paramètres de base.
Texte d'identification de la machine	Le texte à afficher dans la barre de titre du POA. Si vous avez sélectionné **Nom défini** dans le champ **Afficher l'identification de la machine**, vous pouvez entrer le texte dans ce champ de saisie.

Paramètre de stratégie	Explication
Afficher la mention légale	Affiche une zone de texte avec un contenu pouvant être configuré qui apparaît avant l'authentification dans POA. Dans certains pays, la loi exige l'affichage d'une zone de texte ayant un certain contenu. L'utilisateur doit confirmer la zone de texte avant que le système ne continue. Avant de spécifier un texte, ce dernier doit être enregistré en tant qu'élément de texte dans la **zone de navigation de stratégie** sous **Texte d'informations**.
Texte de la mention légale	Le texte à afficher en tant que mention légale. Dans ce champ, vous pouvez sélectionner un élément de texte enregistré dans **Texte d'informations** dans la **zone de navigation de stratégie**.
Afficher des infos supplémentaires	Affiche une zone de texte avec un contenu pouvant être configuré qui apparaît après la mention légale (si elle est activée). Vous pouvez définir si les informations supplémentaires doivent être affichées : ■ Jamais ■ À chaque démarrage système ■ À chaque connexion
Texte des informations supplémentaires	Le texte à afficher en tant qu'informations supplémentaires. Dans ce champ, vous pouvez sélectionner un élément de texte enregistré dans **Texte d'informations** dans la **zone de navigation de stratégie**.
Afficher pendant (sec.)	Dans ce champ, vous pouvez définir la durée (en secondes) pendant laquelle les informations supplémentaires doivent être affichées. Vous pouvez spécifier le nombre de secondes après lesquelles la zone de texte d'informations supplémentaires est fermée automatiquement. L'utilisateur peut fermer la zone de texte à tout moment en cliquant sur **OK**.

Paramètre de stratégie	Explication
Activer et afficher l'icône de la barre d'état système	L'icône de barre d'état de SafeGuard Enterprise permet à l'utilisateur d'accéder rapidement et facilement à l'ensemble des fonctions de l'ordinateur final. En outre, des informations concernant l'état de l'ordinateur final (nouvelles stratégies reçues, ...) peuvent être affichées dans des infobulles. **Oui :** l'icône de barre d'état est affichée dans la zone d'information de barre des tâches et l'utilisateur est continuellement informé via l'infobulle concernant l'état de l'ordinateur final protégé par SafeGuard Enterprise. **Non :** l'icône de barre d'état n'est pas affichée. Aucune information d'état n'est affichée via l'infobulle. **Muet :** l'icône de barre d'état est affichée dans la zone d'information de barre des tâches mais aucune information d'état n'est affichée via l'infobulle.
Afficher les icônes superposées dans l'Explorateur	Définit si des symboles de clé Windows s'affichent pour indiquer l'état de chiffrement des volumes, périphériques, dossiers et fichiers.
Clavier virtuel en POA	Définit si un clavier virtuel peut être affiché sur demande dans la boîte de dialogue de POA pour la saisie du mot de passe.
OPTIONS D'INSTALLATION	
Désinstallation autorisée	Détermine si la désinstallation de SafeGuard Enterprise est autorisée sur les ordinateurs finaux. Lorsque l'option **Désinstallation autorisée** est définie sur ***Non***, SafeGuard Enterprise ne peut pas être désinstallé, même par quelqu'un ayant des droits d'administrateur, lorsque ce paramètre est actif au sein d'une stratégie.
PARAMÈTRES D'INFRASTRUCTURE DE BASE CRYPTOGRAPHIQUE	
Boîtes à outils cryptographiques Windows	Options possibles : ■ Moteur cryptographique SafeGuard ■ Support TPM AET SafeSign : générateur matériel de nombres aléatoires ; nécessite une carte principale spéciale dans le PC.

Paramètre de stratégie	Explication
PARAMÈTRES DE SUPPORT DE CLÉ CRYPTOGRAPHIQUE POUR LE MODULE 1 PKCS#11	
Nom du module	Enregistre le module PKCS#11 d'une clé cryptographique. Les options suivantes sont disponibles : ■ Siemens CardOS API ■ AET SafeSign Identity Client ■ Charismathics Smart Security Interface ■ Aladdin eToken PKI Client ■ RSA Authentication Client 2.x ■ RSA Smart Card Middleware 3.x ■ ActivIdentity ActivClient ■ a.sign Client ■ Gemalto .NET Card ■ Gemalto Classic Client ■ Gemalto Access Client ■ IT Solution trustWare CSP+ ■ Estonian ID Card ■ NetKey 3.0

Paramètre de stratégie	Explication
	Informations de licence pour Siemens et Charismatics : Sachez que l'utilisation du middleware respectif pour le système d'exploitation standard requiert un contrat de licence avec Siemens Medical/Charismatics. Pour obtenir des licences, renseignez-vous à l'adresse suivante : ■ Global Siemens Healthcare Headquarters Siemens AG Healthcare Sector Henkestrasse 127 D-91052 Erlangen Allemagne Tél.: +49 69 797 6602 ■ *http://www.charismathics.com/cryptoshop/shop_content.php* ou à l'adresse sales@charismathics.com
Services en attente de	Ce paramètre permet de résoudre les problèmes de certaines cartes à puce. Notre support fournira les paramètres correspondants requis.

16 SafeGuard Configuration Protection

Les réseaux d'entreprise actuels sont caractérisés par une prolifération de ports informatiques facilement accessibles comme USB, FireWire et PCMCIA. Une variété d'adaptateurs de communication (comme Bluetooth, IrDA et WLAN) et de types de périphériques (comme des dispositifs de stockage, des imprimantes, des appareils photo numériques, des smartphones et des PDA) permettent également d'accéder facilement aux points de terminaison via ces ports et périphériques.

Ces périphériques permettent d'obtenir une accessibilité et une productivité optimales mais laissent les points de terminaison ouverts et sujets à toute infiltration. La quantité de données d'entreprise résidant sur les points de terminaison étant estimée à plus de 60 %, ceux-ci peuvent constituer la partie la plus essentielle, mais également la plus vulnérable, du réseau de l'entreprise.

L'informatique d'entreprise actuelle vise à établir un compromis entre productivité et sécurité. Les besoins des entreprises en termes de productivité les poussent à adopter de nouveaux périphériques et concepts de sécurité. Elles doivent cependant maintenir des mesures de précaution extrêmes contre les fuites, vols, fraudes, infections de virus et l'utilisation inappropriée des informations et des ressources de manière générale.

Selon la recherche Vista, 70 % des failles de sécurité informatique sont internes à l'entreprise. Les entreprises font ainsi de la sécurité interne, notamment l'accès interne aux ressources réseau, la priorité absolue, même si des solutions de passerelle comme les anti-virus et les pare-feu sont appliquées. Le principal défi actuel relatif à la sécurité des entreprises consiste à fournir un accès aux informations clés sans les exposer à des risques, et également de faire confiance aux utilisateurs internes tout en contrôlant leurs actions afin de vérifier leur fiabilité.

Une véritable protection ne peut être obtenue qu'en développant une « enceinte numérique » autour de chaque ordinateur et en protégeant intelligemment ses ports tout en autorisant judicieusement l'accès aux périphériques approuvés.

16.1 La solution SafeGuard Configuration Protection

Associé à SafeGuard PortAuditor (consultez le *manuel d'utilisation de SafeGuard PortAuditor*), SafeGuard Configuration Protection propose une solution complète qui permet aux organisations de connaître les ports et périphériques utilisés dans leur organisation (**visibilité**), afin de définir une stratégie qui **contrôle** leur utilisation et de **protéger** les données transférées.

SafeGuard Configuration Protection contrôle chaque point de terminaison et chaque périphérique, quel que soit le réseau ou l'interface. Il contrôle le trafic en temps réel et applique des stratégies de sécurité personnalisées et très détaillées sur toutes les interfaces de périphériques sans fil et de stockage, notamment :

1. **Interfaces physiques :**
   a) USB
   b) FireWire
   c) PCMCIA
   d) Secure Digital (SD)
   e) Parallèle
   f) Série
   g) Modem
2. **Sans fil :**
   a) Réseau local sans fil (WLAN)
   b) Bluetooth
   c) Infrarouge (IrDA)
3. **Stockage :**
   a) Périphériques de stockage amovibles
   b) Disques durs externes
   c) Lecteurs de CD/DVD
   d) Lecteurs de disquettes
   e) Lecteurs de bandes

SafeGuard Configuration Protection détecte et active une restriction de périphérique par type, modèle, voire numéro de série de périphérique. En ce qui concerne les périphériques de stockage, SafeGuard Configuration Protection permet à un responsable de la sécurité de bloquer

totalement tous les périphériques de stockage. Les commandes WLAN sont basées sur l'adresse MAC, le SSID ou le niveau de sécurité du réseau.

16.1.1 Fonctions

1. **Contrôle du port :** SafeGuard Configuration Protection permet d'autoriser, de bloquer ou de restreindre intelligemment l'utilisation de tout ou partie des ports d'ordinateur de votre organisation en fonction de l'ordinateur utilisé, de l'utilisateur connecté et/ou du type de port. SafeGuard Configuration Protection contrôle : les ports USB, PCMCIA, FireWire, Secure Digital, Série, Parallèle, Modem (numérotation, 3G, etc.), WLAN, IrDA et Bluetooth.

2. **Contrôle du périphérique** : identification et approbation très précises des périphériques, incluant une liste complète des types de périphériques et une liste blanche fiable de modèles de périphériques, voire de périphériques distincts (par numéro de série).

3. **Contrôle du stockage :** contrôle spécial des périphériques de stockage externes et internes, notamment les supports amovibles, disques durs externes, CD/DVD, lecteurs de disquettes et de bandes. La stratégie peut bloquer l'utilisation de types, modèles de périphériques, voire de périphériques distincts (par numéro de série).

4. **Bloquer le pontage de réseau hybride :** SafeGuard Configuration Protection permet aux responsables de la sécurité de contrôler et d'empêcher l'utilisation simultanée de divers protocoles réseau pouvant entraîner un pontage de réseau hybride involontaire ou volontaire (comme le pontage WLAN et le pontage de carte 3G). La configuration de clients SafeGuard Configuration Protection dans le but de bloquer l'accès à des liens WLAN, Bluetooth, Modems ou IrDA, alors que l'interface réseau TCP/IP filaire principale est connectée à un réseau, permet aux utilisateurs d'exploiter divers protocoles réseau lorsqu'ils sont déconnectés du réseau uniquement (empêchant ainsi la création et l'utilisation abusive d'un pont de réseau hybride).

Avis : les ports internes comme des bus de stockage IDE, SCSI, ATA et S-ATA par exemple, utilisés pour connecter des lecteurs de disque dur interne ainsi que PCI et PCI-X, sont autorisés par défaut.

5. **Bloquer les enregistreurs de frappe matériels USB et PS/2 :** bloquer des enregistreurs de frappe matériels USB qui peuvent collecter et enregistrer chaque frappe sur vos points de terminaison et rendre des enregistreurs de frappe matériels PS/2 inutiles.

6. **Messages utilisateur final :** lorsque le client SafeGuard Configuration Protection applique des stratégies sur un ordinateur final, un message s'affiche pour l'utilisateur afin de l'informer des ports et périphériques bloqués.

16.2 Protection via SafeGuard Configuration Protection

SafeGuard Configuration Protection protège vos points de terminaison comme suit :

16.2.1 Contrôle du port

SafeGuard Configuration Protection permet d'autoriser, de bloquer ou de restreindre intelligemment l'utilisation de tout ou partie des ports d'ordinateur de votre organisation en fonction de l'ordinateur utilisé, de l'utilisateur connecté et/ou du type de port. SafeGuard Configuration Protection contrôle : les ports USB, PCMCIA, FireWire, Secure Digital, Série, Parallèle, Modem (numérotation, 3G, etc.), WLAN, IrDA et Bluetooth.

Un port bloqué est indisponible, comme si ses câbles étaient coupés. L'indication d'un port bloqué est fournie au démarrage de l'ordinateur ou lorsqu'une stratégie appliquée désactive un port précédemment autorisé.

16.2.2 Contrôle du périphérique

Outre le contrôle de l'accès au port, SafeGuard Configuration Protection propose un autre niveau de précision en vous permettant de définir les périphériques pouvant accéder à un port.

En ce qui concerne les ports USB, PCMCIA et FireWire, vous pouvez définir les types de périphériques, les modèles de périphériques et/ou les périphériques distincts pouvant accéder à un port, comme suit :

- **Types de périphériques :** cette option vous permet de restreindre l'accès à un port en fonction du type de périphérique qui y est connecté. Les types de périphériques sont, par exemple, les périphériques d'impression, les adaptateurs réseau, les périphériques d'interface humaine (une souris par exemple) ou les périphériques d'imagerie.
  Les types de périphériques pouvant être sélectionnés sont intégrés à SafeGuard Configuration Protection.
  Pour autoriser un périphérique ne figurant pas dans cette liste de types, vous pouvez utiliser l'option **Modèles** ou **Périphériques distincts**, décrite ci-dessous.
- **Modèles :** cette option représente le modèle d'un type de périphérique spécifique, toutes les imprimantes HP ou toutes les cartes mémoire USB
  M-Systems par exemple.
- **Périphériques distincts :** cette option fait référence à une liste de périphériques distincts, chacun disposant d'un numéro de série unique, indiquant qu'il s'agit d'un périphérique spécifique. Par exemple : le PDA du directeur général peut être autorisé et tous les autres PDA bloqués.

Protection contre les enregistreurs de frappe matériels

Les enregistreurs de frappe matériels sont des périphériques pouvant être placés par une entité hostile entre un clavier et son ordinateur hôte afin de collecter et d'enregistrer une saisie au clavier et de dérober des informations critiques, notamment l'identité et le mot de passe.

Grâce à SafeGuard Configuration Protection, vous pouvez protéger vos utilisateurs contre cette menace : SafeGuard Configuration Protection peut détecter des enregistreurs de frappe matériels connectés à un port USB ou PS/2 et votre stratégie peut spécifier le blocage ou non des enregistreurs de frappe lorsqu'ils sont détectés.

16.2.3 Contrôle du stockage

Le contrôle du stockage propose un niveau de détails supplémentaire dans lequel vous spécifiez les exigences de sécurité de votre organisation. Ceci peut s'appliquer à tous les périphériques de stockage, internes ou externes, fixes ou amovibles. Vous pouvez bloquer totalement les périphériques de stockage.

Comme pour les périphériques hors stockage, décrits dans la section précédente, les périphériques de stockage peuvent également être approuvés en fonction de leur type, modèle ou ID unique.

Contrôle du lancement automatique

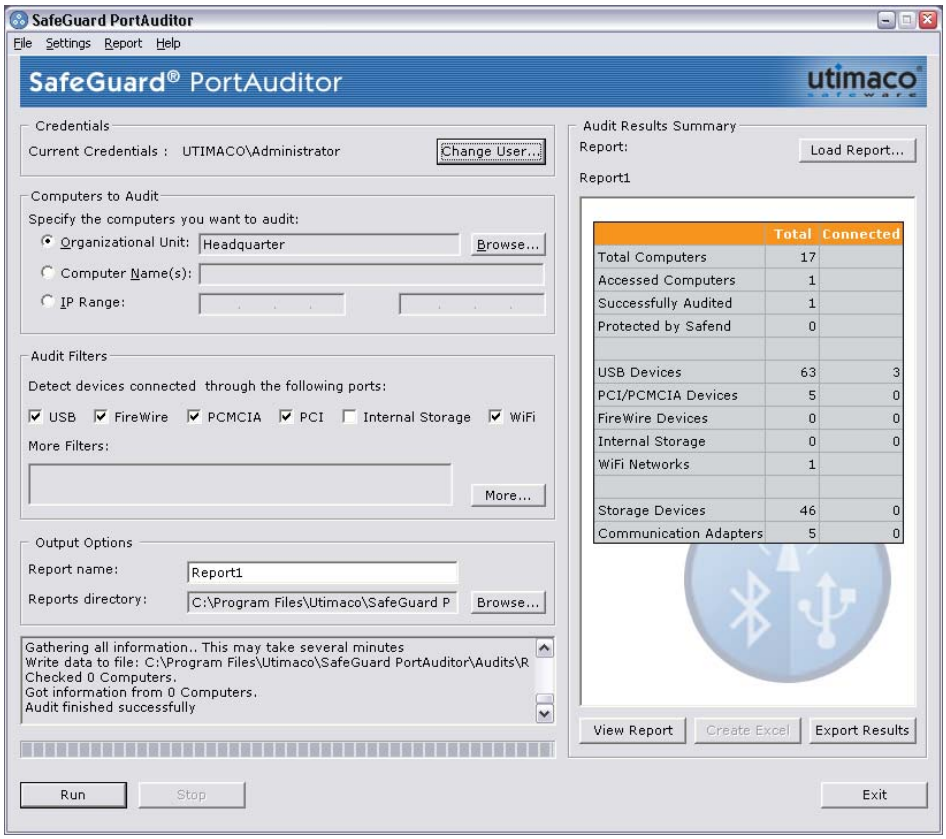
Grâce à SafeGuard Configuration Protection, vous pouvez permettre à vos utilisateurs finals d'utiliser leurs nouveaux périphériques de stockage tout en vous assurant que vos points de terminaison ne sont pas exposés à d'éventuelles menaces et applications à risques pouvant résider sur ces périphériques. Vous pouvez bloquer facilement les tâches de lancement automatique dans le cadre de votre stratégie de sécurité. Grâce à notre technologie client précise et unique, vous pouvez autoriser l'utilisation de périphériques de stockage intelligents et bloquer uniquement leur fonction de lancement automatique pouvant présenter une menace.

16.2.4 Contrôle du réseau local sans fil (WLAN)

Le contrôle du WLAN garantit que les utilisateurs ne se connectent qu'aux réseaux approuvés. Vous pouvez spécifier les réseaux ou liens ad hoc dont l'accès est autorisé. Vous pouvez spécifier l'adresse MAC des points d'accès, le SSID du réseau, la méthode d'authentification et les méthodes de chiffrement pour définir les liens approuvés.

16.2.5 SafeGuard PortAuditor

Bien que ne faisant pas partie de la solution SafeGuard Configuration Protection, SafeGuard PortAuditor est un outil coopérant avec SafeGuard Configuration Protection et qui le complète pour vous proposer une vue d'ensemble des ports, périphériques et réseaux qui sont (ou étaient) utilisés par les utilisateurs de votre organisation. Utilisez le résultat d'une analyse SafeGuard PortAuditor pour sélectionner les périphériques et réseaux dont vous souhaitez approuver l'utilisation.



Pour plus de détails, consultez le *manuel d'utilisation de SafeGuard PortAuditor*.

16.3 Stratégies de protection de la configuration

Une stratégie de protection de la configuration spécifie les ports autorisés, bloqués ou restreints. **Restreint** signifie que seuls les types de périphériques, modèles de périphériques, périphériques distincts ou connexions WLAN spécifiés peuvent accéder via ce port.

Une stratégie spécifie les autorisations d'accès des types de périphériques de stockage, des modèles de périphériques de stockage et des périphériques de stockage distincts, ainsi que des connexions WLAN, vous permettant ainsi de spécifier s'ils sont autorisés, bloqués ou restreints (comme pour les périphériques).

Une stratégie peut également bloquer des **enregistreurs de frappe matériels** connectés à un port USB ou PS/2. Les enregistreurs de frappe matériels sont des périphériques pouvant être placés sur une entité hostile entre un clavier et son ordinateur hôte afin de consigner la saisie au clavier. Votre stratégie peut spécifier si les enregistreurs de frappe matériels doivent être bloqués lorsqu'ils sont détectés par SafeGuard Configuration Protection.

SafeGuard Configuration Protection adopte une approche de sécurité positive, ce qui signifie que tous les périphériques sont autorisés, à moins que vous ne définissiez une stratégie bloquant leur accès.

La définition d'une stratégie est décrite dans les sections suivantes.

16.3.1 Définition de stratégies de configuration de la protection : flux de travail

Vous trouverez ci-après une présentation du flux de travail de définition d'une nouvelle stratégie. Chacune des étapes est décrite plus en détail dans une sous-section.

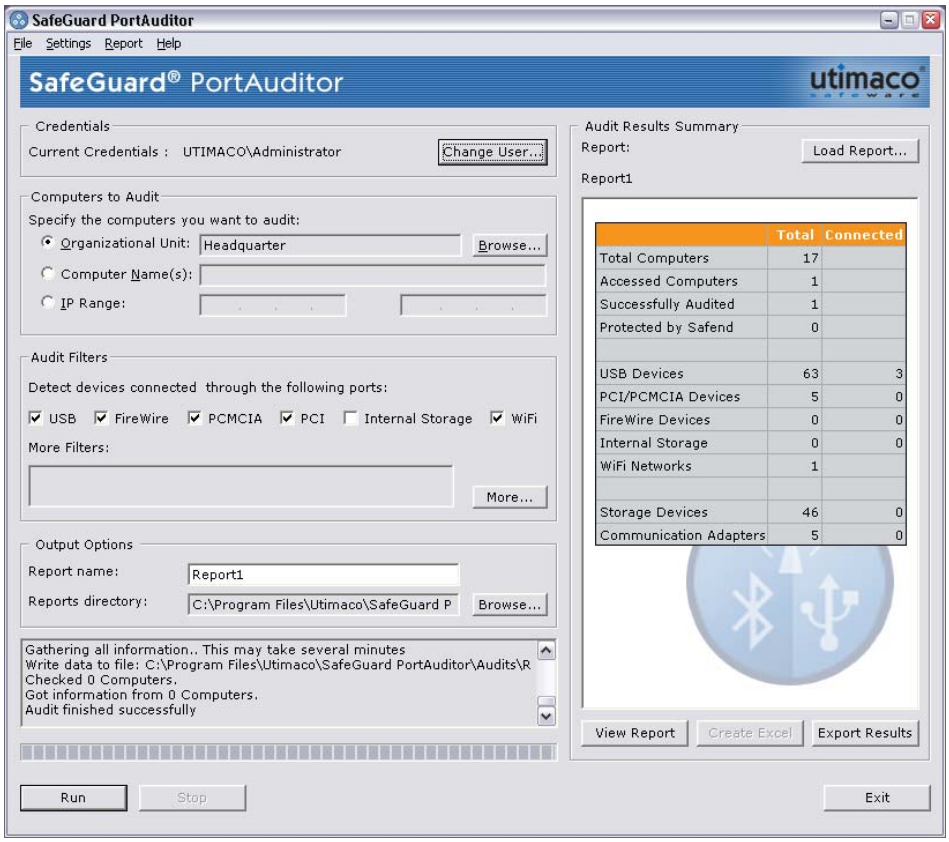
Le flux de travail suggère un ordre simple et immédiat d'exécution des étapes que vous pouvez changer selon votre choix.

- ***Étape 1 : Analyser les ordinateurs et détecter l'utilisation du port/périphérique/réseau local sans fil (WLAN)*** : utilisez SafeGuard PortAuditor pour analyser les ordinateurs du réseau afin de détecter les périphériques et réseaux locaux sans fil actuellement et précédemment connectés (comme indiqué dans le registre de l'ordinateur), tel que décrit dans le *manuel d'utilisation de SafeGuard PortAuditor*. Vous utiliserez ces informations lors de la définition d'une stratégie afin de spécifier les ports et périphériques autorisés, bloqués ou restreints.
- ***Étape 2 : Planifier la stratégie*** décrit les informations à collecter pour planifier correctement la meilleure stratégie de protection de point de terminaison pour votre organisation.
- ***Étape 3 : Créer une stratégie*** décrit comment créer une nouvelle stratégie. Vous pouvez créer autant de stratégies que nécessaire, une pour l'ensemble de l'organisation et une autre pour chaque groupe d'ordinateurs ou d'utilisateurs.

- ***Étape 4 : Définir le contrôle du port*** décrit comment définir le contrôle du port de votre stratégie, à savoir les ports autorisés, bloqués et restreints utilisés par certains périphériques uniquement. Cette section décrit également comment empêcher un pontage de réseau hybride.
- ***Étape 5 : Définir le contrôle du périphérique*** décrit comment définir plus particulièrement les périphériques autorisés à se connecter via les ports restreints de vos points de terminaison.
- ***Étape 6 : Définir le contrôle du stockage*** décrit comment définir plus particulièrement les périphériques de stockage autorisés à se connecter aux points de terminaison.
- ***Étape 7 : Définir le contrôle du réseau local sans fil (WLAN)*** décrit comment définir les connexions WLAN approuvées.
- ***Étape 8 : Définir le contrôle du fichier*** décrit comment définir les autorisations des types de fichiers transférés de/vers des périphériques de stockage.
- ***Étape 9 : Enregistrer et publier la stratégie*** décrit les options d'enregistrement de la stratégie dans la base de données de stratégies et de publication afin que celle-ci puisse être associée aux ordinateurs finaux correspondants.

16.3.2 Étape 1 : Analyser les ordinateurs et détecter l'utilisation du port/ périphérique/réseau local sans fil (WLAN)

Bien que ne faisant pas partie de la solution SafeGuard Configuration Protection, SafeGuard PortAuditor est un outil coopérant avec SafeGuard Configuration Protection et qui le complète pour vous proposer une vue d'ensemble des ports, périphériques et réseaux qui sont (ou étaient) utilisés par les utilisateurs de votre organisation. Utilisez le résultat d'une analyse SafeGuard PortAuditor pour sélectionner les périphériques et réseaux dont vous souhaitez approuver l'utilisation.



16.3.3 Étape 2 : Planifier la stratégie

Avant de définir votre stratégie, prenez le temps de la planifier pour qu'elle convienne le mieux à votre organisation. La meilleure stratégie SafeGuard Configuration Protection pour votre organisation est celle répondant à ses besoins spécifiques tout en respectant les exigences des personnes ayant accès, via les ports, aux ordinateurs de votre organisation.

La première chose à planifier concerne les types d'OU (unités organisationnelles) et de groupes auxquels les stratégies s'appliqueront.

Stratégies utilisateur et ordinateur

Par défaut, SafeGuard Configuration Protection utilise des groupes d'utilisateurs et des groupes d'ordinateurs contrôlés par Active Directory. Chaque option présente des avantages propres, comme décrit ci-dessous.

- **Par groupes d'utilisateurs :** la définition de vos stratégies par groupes d'utilisateurs vous permet de spécifier les autorisations de chaque utilisateur.
  Les stratégies s'appliquant aux utilisateurs remplacent celles s'appliquant aux ordinateurs.
  Si vous choisissez de gérer votre organisation en attribuant des stratégies aux groupes d'utilisateurs, nous recommandons de définir une ou plusieurs stratégies générales pour les ordinateurs. Ceci permet de protéger chaque port d'ordinateur, même si aucun utilisateur n'y est connecté.
  La combinaison de stratégies utilisateur et ordinateur signifie que, par exemple, vous pouvez bloquer des périphériques de stockage USB sur tous les ordinateurs du service clientèle mais que vous pouvez autoriser le responsable du service à appliquer une stratégie plus stricte en fonction de ses nom d'utilisateur et mot de passe, quel que soit l'ordinateur sur lequel il se connecte.

- **Par groupes d'ordinateurs :** la définition de vos stratégies par ordinateurs active la protection des points de terminaison des ordinateurs de votre organisation, quel que soit l'utilisateur connecté.

SafeGuard Configuration Protection applique les stratégies comme suit : il applique tout d'abord une stratégie utilisateur, si elle existe pour l'utilisateur actuellement connecté. Dans le cas contraire, SafeGuard Configuration Protection recherche une stratégie qui s'applique à l'ordinateur et l'utilise, le cas échéant. Cela signifie que, lorsqu'aucun utilisateur n'est connecté, la stratégie liée à l'ordinateur est utilisée. Il est ainsi conseillé de distribuer des stratégies basées sur l'utilisateur afin qu'un utilisateur dispose de la même stratégie quel que soit l'ordinateur auquel il se connecte et de définir des stratégies basées sur l'ordinateur plus restrictives. Ces stratégies basées sur l'ordinateur doivent accorder l'accès aux périphériques, comme une souris et un clavier, à utiliser lorsqu'aucun utilisateur ou un utilisateur externe au domaine ne se connecte.

La configuration initiale du client SafeGuard Configuration Protection autorise toutes les activités de port et de périphérique. Aucun élément n'est donc bloqué. Une configuration permissive est nécessaire afin que toutes les activités de port ne soient pas bloquées automatiquement après l'installation du client SafeGuard Configuration Protection.

Cela signifie que, jusqu'à ce que vous définissiez et distribuiez des stratégies aux points de terminaison (par utilisateur ou par ordinateur), le fonctionnement de la machine sur laquelle le client SafeGuard Configuration Protection vient d'être installé est inchangé (aucun blocage de ports ni de périphériques).

Avis : la stratégie machine est utilisée comme stratégie de secours lorsque la stratégie utilisateur ne peut pas être utilisée ou est falsifiée. Il est donc recommandé de créer une stratégie machine et une stratégie utilisateur, cette dernière étant plus stricte.

Avis : en fonction de l'ordinateur final, quelques secondes peuvent être nécessaires pour l'application d'un changement de stratégie par le client SafeGuard Configuration Protection après la connexion. Cela signifie que lorsque la stratégie machine est plus restrictive que la stratégie utilisateur, l'accès aux périphériques par l'utilisateur peut demander quelques secondes.

16.3.4 Étape 3 : Créer une stratégie

Les stratégies sont créées comme décrit pour toutes les autres stratégies.

16.3.5 Étape 4 : Définir le contrôle du port

Cette étape inclut la configuration d'autorisations de port ainsi que des autorisations de pontage de réseau hybride.

Autorisations de port

SafeGuard Configuration Protection permet une sécurité positive en autorisant l'accès à tous les ports de tous les ordinateurs auxquels une stratégie est distribuée, sauf si cette stratégie spécifie que l'accès à ce port est bloqué, comme suit. Pour chaque port (USB, FireWire, PCMCIA, Secure Digital, Série, Parallèle, Modem, WLAN, IrDA ou Bluetooth), vous pouvez spécifier les options suivantes :

- **Autoriser :** cette option spécifie que le port peut être utilisé à toutes fins, sans restriction sur ce canal de communication.
- **Bloquer :** cette option signifie qu'aucun accès n'est possible via ce port. Le port est indisponible, comme si ses câbles étaient coupés.

- **Restreindre :** pour les ports USB, FireWire, PCMCIA et WLAN, vous pouvez également spécifier que l'accès aux ports de ce type est restreint. Un paramètre **Restreint** vous permet de définir plus particulièrement (à savoir plus précisément) les périphériques ou connexions autorisés à accéder au port. Par exemple, vous pouvez spécifier que seul l'accès des périphériques USB d'un modèle spécifique, voire des périphériques USB spécifiques (des périphériques distincts avec un numéro de série unique), est autorisé. Pour les ports physiques, ceci peut être effectué via l'option **Contrôle du périphérique** décrite à l'*Étape 5 : Définir le contrôle du périphérique* et via l'option **Contrôle du stockage** décrite à l'*Étape 6 : Définir le contrôle du stockage*. Pour les ports sans fil, ceci est effectué via l'option **Contrôle du réseau local sans fil (WLAN)** décrite à l'*Étape 8 : Définir le contrôle du réseau local sans fil (WLAN)*.

Avis : le contrôle du périphérique et le contrôle du réseau local sans fil (WLAN) d'une stratégie ne s'appliquent qu'aux ports restreints.
Le contrôle du stockage d'une stratégie s'applique aux ports restreints et autorisés.

Pour chaque port, spécifiez si le type d'action est **Autoriser**, **Bloquer** ou **Restreindre** en sélectionnant l'option appropriée dans le menu déroulant.

Avis : les ports internes comme des bus de stockage IDE, SCSI, ATA et S-ATA par exemple, utilisés pour connecter des lecteurs de disque dur interne ainsi que PCI et PCI-X, sont autorisés par défaut.

Avis : les paramètres SecureDigital dans la section *Ports physiques* sont applicables lorsque SecureDigital est utilisé comme un port. Lorsque SecureDigital est connecté via un adaptateur USB, il devient un périphérique de stockage de masse USB. Si SecureDigital est connecté directement au PC ou au portable, la reconnaissance dépend du modèle de PC ou de portable.

Autorisations de pontage de réseau hybride

SafeGuard Configuration Protection permet aux administrateurs de contrôler et d'empêcher l'utilisation simultanée de divers protocoles réseau pouvant entraîner un pontage de réseau hybride involontaire ou volontaire (comme le pontage WLAN et le pontage de carte 3G). La configuration de clients SafeGuard Configuration Protection dans le but de bloquer l'accès à des liens WLAN, Bluetooth, Modems ou IrDA, alors que l'interface réseau TCP/IP filaire principale est connectée à un réseau, permet aux utilisateurs d'exploiter certains protocoles réseau lorsqu'ils sont déconnectés du réseau uniquement (empêchant ainsi la création et l'utilisation abusive d'un pont de réseau hybride).

Les autorisations de pontage de réseau hybride sont définies dans la section *Pontage de réseau anti-hybride*.

16.3.6 Étape 5 : Définir le contrôle du périphérique

Dans la section *Contrôle du port*, pour les ports USB, FireWire et PCMCIA, vous pouvez spécifier que l'accès aux ports de ces types est restreint (ceci s'applique aux ports WLAN également, comme décrit à l'*Étape 8 : Définir le contrôle du réseau local sans fil (WLAN)*). Sélectionnez **Restreindre** pour définir plus particulièrement, via la section **Contrôle du périphérique**, les périphériques autorisés à accéder à ces ports.

La section *Contrôle du périphérique* vous permet de spécifier les types de périphériques dont l'accès est autorisé et à attribuer la *Liste blanche* correspondante utilisée pour spécifier les modèles de périphériques ou les périphériques distincts dont l'accès est autorisé. Si un périphérique n'est pas défini comme autorisé tel que décrit ci-dessous, il est alors bloqué. La notion de contrôle du périphérique d'une stratégie s'applique à **tous** les ports **restreints**.

Contrôle du périphérique – Paramètres

- **Tous les périphériques** (zone supérieure) : dans cette zone, vous pouvez **Autoriser**, **Restreindre** ou **Bloquer** l'accès à tous les types de périphériques.
  Si vous sélectionnez **Autoriser** ou **Bloquer** pour **Tous les périphériques**, la partie restante de la section est désactivée.
  Vous pouvez également **Autoriser** ou **Bloquer** les enregistreurs de frappe matériels.

- **Types de périphériques** (zone centrale) : si vous avez sélectionné l'option **Restreindre** pour *Tous les périphériques* comme décrit dans le paragraphe précédent, cette option vous permet d'autoriser ou de restreindre l'accès à un périphérique en fonction de son type. Par exemple : Périphériques d'impression, Adaptateurs réseau ou Périphériques d'imagerie.

  Les types de périphériques pouvant être sélectionnés sont intégrés à SafeGuard Configuration Protection. Pour autoriser un périphérique dont le type ne figure pas dans la liste, ajoutez-le à la liste de périphériques approuvés (la **Liste blanche**) à l'aide de l'option **Modèle approuvé** ou **Périphériques distincts** comme décrit ci-dessous. Une description des types de périphériques pris en charge est proposée dans *Types de périphériques pris en charge*.

- **Périphériques inconnus** (zone inférieure) : cette option vous permet de déterminer si l'accès aux périphériques inconnus est accordé ou non.

Contrôle du périphérique - Liste blanche

Cette section permet d'attribuer une liste blanche pour les modèles de périphériques et/ou une liste blanche pour les périphériques distincts :

- **Liste blanche pour les modèles de périphériques** : cette option fait référence au modèle d'un type de périphérique spécifique, comme un modèle spécifique d'imprimante HP, la LaserJet 4050N par exemple. Spécifiez un fichier de liste blanche contenant ces périphériques.
- **Liste blanche pour les périphériques distincts** : cette option fait référence aux périphériques distincts avec un numéro de série unique, à savoir un réel périphérique spécifique. Spécifiez un fichier de liste blanche contenant ces périphériques. Par exemple : l'imprimante personnelle du directeur général peut être autorisée à se connecter alors que d'autres périphériques d'impression ne le sont pas.

Avis : cette section est désactivée lorsque vous sélectionnez **Autoriser** ou **Bloquer** dans l'option *Tous les périphériques*. Consultez *Définition du contrôle du périphérique*.

Avis : lorsqu'un périphérique fait partie de plusieurs groupes et que ces groupes disposent des mêmes autorisations, SafeGuard Configuration Protection choisit arbitrairement entre les groupes.

Définition du contrôle du périphérique

1. Dans l'option *Tous les périphériques*, spécifiez dans le menu déroulant si *Tous les périphériques* sont **autorisés**, **restreints** ou **bloqués**.

Avis : sélectionnez **Autoriser** ou **Bloquer** lorsque vous ne souhaitez pas appliquer un contrôle du périphérique détaillé à ce moment précis. Utilisez également cette option lorsque vous souhaitez remplacer des définitions détaillées existantes mais que vous souhaitez les restaurer ultérieurement.

2. Si vous sélectionnez **Autoriser** ou **Bloquer** pour *Tous les périphériques***,** aucune autre action n'est nécessaire dans la section *Contrôle du périphérique* et vous pouvez passer à l'*Étape 6 : Définir le contrôle du stockage*.

3. Si vous avez sélectionné **Restreindre** pour *Tous les périphériques*, spécifiez si les enregistreurs de frappe matériels sont **autorisés** ou **bloqués**.

Avis : si le client SafeGuard Configuration Protection suspecte qu'un enregistreur de frappe matériel USB est connecté au clavier et que les enregistreurs de frappe sont **bloqués**, le clavier l'est également. Pour activer le clavier, conseillez à l'utilisateur de le connecter directement à l'ordinateur.

Avis : lorsque vous bloquez les enregistreurs de frappe matériels, les enregistreurs de frappe USB et PS/2 sont bloqués. Lorsque le client SafeGuard Configuration Protection vous protège contre les enregistreurs de frappe PS/2, aucun message utilisateur ne s'affiche. L'enregistreur de frappe est néanmoins inutile étant donné que les informations qu'il capture sont brouillées.
Notez également que lorsqu'un enregistreur de frappe PS/2 est bloqué et que vous utilisez un commutateur écran-clavier-souris PS/2, le changement de commutateur entre ordinateurs ne fonctionne pas à partir du clavier. Vous pouvez changer d'ordinateur en appuyant directement sur le commutateur.

4. Si vous avez sélectionné **Restreindre** pour *Tous les périphériques*, définissez les autorisations de chaque **type de périphérique** dans la section *Types de périphériques* comme suit :

   a) **Autoriser :** autorise tous les périphériques de ce type.

   b) **Restreindre :** tous les périphériques sont bloqués sauf s'ils sont explicitement approuvés dans la *Liste blanche* décrite dans *Approbation de périphériques et de connexions WLAN*.

5. Sélectionnez la **Liste blanche pour les modèles de périphériques** et la **Liste blanche pour les périphériques distincts** pour les ajouter aux périphériques autorisés dans la *Liste blanche* comme décrit dans Listes blanches - *Approbation de périphériques et de connexions WLAN*.

16.3.7 Étape 6 : Définir le contrôle du stockage

Les périphériques de stockage sont généralement les principales sources de fuite d'informations dans une organisation.

SafeGuard Configuration Protection vous permet de contrôler l'accès en autorisant un accès total ou en bloquant tout périphérique identifié comme un périphérique de stockage. Ceci inclut les supports amovibles comme les cartes mémoire USB, les appareils photo numériques, etc., ainsi que les périphériques traditionnels comme les lecteurs de disquettes, les lecteurs de CD/ DVD, les disques durs externes et les lecteurs de bandes.

La notion de contrôle du stockage d'une stratégie est appliquée sur tous les ports auxquels un périphérique de stockage peut se connecter. Ceci inclut les ports **autorisés** ou **restreints** ainsi que les ports non protégés par SafeGuard Configuration Protection. Sur un port **bloqué**, tous les périphériques de stockage sont bloqués étant donné que bloquer un port équivaut à débrancher ses câbles.

Avis : les attaques et les fuites directes via des disques durs internes n'étant pas fréquentes, SafeGuard Configuration Protection ne gère pas le blocage ou la restriction de ces lecteurs afin de ne pas interrompre les tâches en cours.

Contrôle du stockage – Paramètres

Cette section inclut les zones suivantes :

1. **Tous les périphériques de stockage** : dans cette zone, vous pouvez **Autoriser**, **Restreindre** ou **Bloquer** l'accès à tous les périphériques de stockage. Si vous sélectionnez **Autoriser** ou **Bloquer** pour **Tous les périphériques de stockage**, la partie restante de la section est désactivée.
   Vous pouvez également choisir d'autoriser ou de bloquer la fonction d'exécution automatique de certains périphériques de stockage comme les CD/DVD.

2. **Types de stockages** : si vous avez sélectionné l'option **Restreindre** pour *Tous les périphériques de stockage*, cette option vous permet d'autoriser ou de restreindre l'accès à un périphérique de stockage en fonction de son type. Par exemple : périphériques amovibles ou lecteurs de CD/DVD. Les types de périphériques pouvant être sélectionnés sont intégrés à SafeGuard Configuration Protection et incluent les options et types suivants :

   a) **Supports amovibles :** s'applique à tous les périphériques de stockage plug-and-play comme les cartes mémoire USB, appareils photos numériques, lecteurs MP3 portables, etc.

   b) **Autoriser les fonctions intelligentes des supports amovibles :** définissez cette option sur **Autoriser** pour permettre l'utilisation de supports amovibles mettant en œuvre la fonction intelligente. Définissez cette option sur **Bloquer** pour empêcher la fonction intelligente de tels périphériques d'être mise en œuvre.

   c) Disques durs externes

   d) Lecteurs de CD/DVD

   e) Lecteurs de disquettes

   f) Lecteurs de bandes

Les supports amovibles, disques durs externes, lecteurs de CD/DVD et lecteurs de disquettes peuvent également être définis en **Lecture seule**.

Utilisez la *Liste blanche* pour approuver l'utilisation de **modèles de stockage** ou de **périphériques de stockage distincts** spécifiques.
Une description des types de périphériques pris en charge est proposée dans *Types de périphériques pris en charge*. Pour obtenir une procédure de définition des options de cette section, consultez *Définition du contrôle du stockage*.

Contrôle du stockage – Liste blanche

Cette section permet d'attribuer une liste blanche pour les modèles de périphériques de stockage et/ou une liste blanche pour les périphériques de stockage distincts :

1. **Liste blanche pour les modèles de périphériques de stockage** : cette option fait référence au modèle d'un type de périphérique de stockage spécifique comme un modèle de carte mémoire USB spécifique.

2. **Liste blanche pour les périphériques de stockage distincts** : périphériques de stockage distincts avec un numéro de série unique, à savoir un périphérique existant et spécifique. Par exemple : la carte mémoire USB personnelle du directeur général peut être autorisée à se connecter alors que d'autres cartes mémoire USB ne le sont pas.

Avis : cette section est désactivée lorsque vous sélectionnez l'option **Autoriser** ou **Bloquer** pour *Tous les périphériques de stockage*.

Avis : sélectionnez **Autoriser** ou **Bloquer** lorsque vous ne souhaitez pas appliquer un contrôle du périphérique de stockage détaillé à ce moment précis mais que vous envisagez d'en définir un ultérieurement. Utilisez également cette option lorsque vous souhaitez remplacer des définitions détaillées existantes mais que vous souhaitez les restaurer ultérieurement.

16.3.8 Étape 7 : Définir le contrôle du réseau local sans fil (WLAN)

Outre les périphériques, SafeGuard Configuration Protection contrôle et surveille vos connexions WLAN pour garantir que les ordinateurs finaux n'utilisent que des connexions autorisées et sécurisées. Dans la section *Contrôle du port*, vous pouvez spécifier que l'accès à un port WLAN soit **restreint**. Sélectionnez **Restreint** pour définir plus particulièrement, via la section *Types de connexions WLAN*, les réseaux autorisés à accéder à ce port.

Avis : lors de la restriction d'utilisation du réseau local sans fil en tant que port, SafeGuard Configuration Protection contrôle et régule les connexions WLAN sur l'infrastructure Microsoft WZC. Tout pilote de périphérique tentant d'accéder à la carte réseau sans utiliser WZC sera bloqué.

Si vous utilisez plusieurs cartes WLAN appliquant des pilotes propriétaires, vous pouvez uniquement **autoriser** ou **bloquer** le réseau local sans fil en tant que port.

Contrôle du réseau local sans fil (WLAN) – Paramètres

Types de connexions WLAN : cette option vous permet d'**autoriser** ou de **restreindre** l'accès aux réseaux locaux sans fil et d'**autoriser** ou de **bloquer** des connexions poste à poste de réseau local sans fil. En ce qui concerne les réseaux locaux sans fil, si vous choisissez **Restreindre**, vous pouvez en outre spécifier les réseaux approuvés.

Contrôle du réseau local sans fil (WLAN) – Liste blanche

Liste blanche pour WLAN : cette option représente les réseaux distincts, notamment leurs propriétés d'authentification et de chiffrement.

Avis : cette section est désactivée si vous sélectionnez l'option **Autoriser** pour les réseaux.

Définition du contrôle du réseau local sans fil (WLAN)

Pour définir le contrôle du réseau local sans fil (WLAN) :

1. Accédez à l'option *WLAN* de la section **Ports sans fil**. Définissez *WLAN* sur **Restreindre**. Ceci active les options situées sous **Types de connexions WLAN**.
2. Dans la section *Types de connexions WLAN*, définissez les autorisations des réseaux *WLAN (Infrastructure)* comme suit :
   a) **Autoriser :** autorise la connexion à tous les réseaux WLAN.
   b) **Restreindre :** tous les réseaux sont bloqués sauf s'ils sont explicitement approuvés dans la *Liste blanche*, comme décrit dans Listes blanches – *Approbation de périphériques et de connexions WLAN*.
3. Dans la section *Types de connexions WLAN*, définissez les autorisations *Peer-to-Peer (Ad Hoc)* (Poste à poste (ad hoc)) comme suit :
   a) **Autoriser :** autorise toutes les connexions WLAN poste à poste.
   b) **Bloquer :** bloque toutes les connexions WLAN poste à poste.

Pour cette option, les autorisations plus précises ne sont pas disponibles.

16.3.9 Étape 8 : Définir le contrôle du fichier

SafeGuard Configuration Protection vous permet de définir des autorisations non seulement pour les périphériques de stockage, mais également pour les fichiers transférés de et vers ces périphériques. Cette opération s'effectue par le contrôle du type de ces fichiers lorsqu'ils sont transférés de/vers des périphériques de stockage externes. Cette technologie permet d'obtenir un classement très précis des fichiers par le biais du contrôle du contenu de l'en-tête du fichier plutôt que par l'utilisation d'extensions, empêchant ainsi les utilisateurs d'outrepasser la protection en modifiant l'extension du fichier.

Le contrôle des fichiers téléchargés sur des périphériques de stockage externes et de ceux chargés sur le point de terminaison protégé présente de nombreux avantages :

- un niveau de protection supplémentaire pour empêcher toute fuite de données ;
- la prévention contre l'introduction de virus/programmes malveillants via des périphériques de stockage externes ;
- la prévention contre l'introduction de contenu inapproprié via des périphériques de stockage externes, par exemple un logiciel sans licence, du contenu sans licence (musique et vidéos, par exemple), du contenu non lié au travail comme des photos privées, etc.

Grâce à cette fonction, vous pouvez définir des stratégies qui approuvent/bloquent des types de fichiers spécifiques sur les canaux d'entrée et de sortie.

Le contrôle du fichier de SafeGuard Configuration Protection comprend les éléments suivants :

- Contrôle du type de fichier : possibilité de contrôler le transfert de fichiers en fonction de leur type.

Le contrôle du fichier s'applique aux périphériques de stockage amovibles, aux disques durs externes et aux CD/DVD.

Contrôle de fichiers – Paramètres

Cette section inclut les zones suivantes :

1. **Types de supports de stockage** : dans cette zone, vous pouvez **Appliquer** le contrôle du type de fichier aux types de stockage ou **Exclure** des types de supports de stockage du contrôle du type de fichier.
   Les types de supports de stockage pouvant être sélectionnés sont intégrés à SafeGuard Configuration Protection et incluent les types suivants :

   a) Lecture de supports amovibles

   b) Écritures sur supports amovibles

   c) Lecture de disques durs externes

   d) Écritures sur disques durs externes

   e) Lecture de CD/DVD

2. Si vous sélectionnez **Appliquer** ou **Exclure** pour au moins l'un des types de supports de stockage, l'autre partie de la section (*Types de fichiers*) est activée. Vous pouvez définir les autorisations suivantes pour chaque type de fichier :

   a) Autoriser

   b) Lecture seule

   c) Écriture

   d) Bloquer
   Les autorisations des types de fichiers s'appliquent à tous les types de supports de stockage auxquels vous avez appliqué le contrôle du fichier dans la section *Types de supports de stockage*.

Le tableau ci-dessous répertorie les types et extensions de fichiers pris en charge par le contrôle du type de fichier de SafeGuard Configuration Protection.

Type de fichier	Extensions	Description
Microsoft Office	DOC	Document Microsoft Word
	DOCX	Document Microsoft Word
	DOCM	Document Microsoft Word
	DOT	Modèle Microsoft Word
	DOTX	Modèle Microsoft Word
	DOTM	Modèle Microsoft Word
	RTF	Format RTF (Rich Text Format)
	PPT	Présentation Microsoft PowerPoint
	PPTX	Présentation Microsoft PowerPoint
	PPTM	Présentation Microsoft PowerPoint
	POT	Modèle Microsoft PowerPoint
	POTX	Modèle Microsoft PowerPoint
	POTM	Modèle Microsoft PowerPoint
	PPS	Diaporama Microsoft PowerPoint
	PPSX	Diaporama Microsoft PowerPoint
	PPSM	Diaporama Microsoft PowerPoint
	PPA	Complément Microsoft PowerPoint
	PPAM	Complément Microsoft PowerPoint
	XLS	Classeur Microsoft Excel

	XLSX	Classeur Microsoft Excel
	XLSM	Classeur Microsoft Excel
	XLSB	Classeur Microsoft Excel
	XLT	Modèle Microsoft Excel
	XLTX	Modèle Microsoft Excel
	XLTM	Modèle Microsoft Excel
	XLA	Complément Microsoft Excel
	XLAM	Complément Microsoft Excel
	MPP	Projet Microsoft Project
	MPT	Modèle Microsoft Project
	VSD	Dessin Microsoft Visio
	VDX	Dessin Microsoft Visio
	VSS	Gabarit Microsoft Visio
	VSX	Gabarit Microsoft Visio
	VST	Modèle Microsoft Visio
	VTX	Modèle Microsoft Visio
	PUB	Microsoft Publisher
	ONE	Sections Microsoft OneNote
	ADP	Projet Microsoft Access
	ADE	Extension de projet Microsoft Access
Documents publiés	PDF	Document Adobe Acrobat
	PS	Document Post Script
	EPS	Format EPS (Encapsulated Post Script)
Pages Web	HTML	Page Web HTML
	HTM	Page Web HTML
	MHT	Page Web archivée
	MHTML	Page Web archivée
	PHP	Script PHP
	HLP	Fichier d'aide Windows
	CHM	Fichier d'aide compilé
	ASP	Page Active Server

	ASPX	Page Web ASP.NET
	ASMX	Services Web ASP.NET
	JHTML	Page Web HTML Java
	JSP	Page Java Server
Images	JPG	Image JPEG
	JPEG	Image JPEG
	GIF	Image GIF
	BMP	Image Bitmap
	DIB	Image indépendante du périphérique
	PNG	Image PNG
	TIF	Format TIFF (Tagged Image Format)
	TIFF	Format TIFF (Tagged Image Format)
	MDI	Fichier Document Imaging Microsoft Office
	JNG	Image JNG
	MNG	Image MNG
	ICO	Icône Windows
	CUR	Curseur Windows
	WMF	Image Métafichier Windows
	EMF	Image Métafichier Windows amélioré
	FH9	Graphiques Macromedia Freehand 9
	JP2	Image JPEG-2000
	PBM	Bitmap Portable
	PGM	Bitmap Portable Graymap
	PPM	Bitmap Portable Pixelmap
	PSD	Graphiques Adobe Photoshop
	CDR	Graphiques vectoriels CorelDRAW
	SVG	Graphiques vectoriels adaptables
Multimédia	WAV	Formes d'ondes audio
	WMA	Audio Windows Media
	MP2	Audio MPEG
	MP3	Audio MPEG

	AIFF	Échange de données audio
	AIF	Échange de données audio
	AU	Audio AU
	RA	Diffusion multimédia en continu RealMedia
	MID	Son numérique d'instrument de musique
	MIDI	Son numérique d'instrument de musique
	RMI	Son numérique d'instrument de musique
	SDS	Échantillon de son numérique d'instrument de musique
	VOC	Audio SoundBlaster Creative Lab
	OGG	Audio codec Ogg Vorbis
	VOX	Audio dialogique
	FLAC	Audio codec sans perte gratuit
	MPEG	Multimédia MPEG
	MPG	Multimédia MPEG
	AVI	Audio vidéo entrelacée
	ASF	Format avancé de diffusion de flux
	WMV	Multimédia Windows Media
	MOV	Clip vidéo QuickTime
	SWF	Fichier d'animation Flash
	FLI	Animation FLIC
	FLC	Animation FLIC
Code de texte et de programme	TXT	Fichier texte
	CSV	Texte formaté (séparé par des virgules)
	PRN	Texte formaté (séparé par des espaces)
	CPP	Code de programme C++
	C	Code de programme C/C++
	H	Fichier d'en-tête C/Java
	XML	Fichier XML
	F	Code de programme FORTRAN
	T90	Code de programme FORTRAN

	MAKEFILE	Fichier de contrôle de compilation
	MAKEFILE.IN	Fichier de contrôle de compilation
	PL1	Code de programme PL1
	ASM	Code de programme en assembleur
	PAS	Code de programme PASCAL
	JAVA	Code de programme JAVA
	M4	Code de programme Meta4
	BCPL	Code de programme BCPL
	CS	Code de programme Visual C#.NET
	PL	Code de programme Perl
	PM	Module de code de programme Perl
	PY	Code de programme Python
	PDB	Base de données de programme Visual C++/ .NET
	BAS	Code de programme BASIC
	VB	Code de programme Visual Basic
	VBS	Script VBScript
	JS	Code source JavaScript
Exécutables	EXE	Exécutable
	DLL	Bibliothèque de liens dynamiques
	PIF	Fichier d'information de programme Windows
	BAT	Lot
	COM	Commande
	OCX	Extension de contrôle OLE (Object Linking and Embedding) ActiveX
	CMD	Commande
	CPL	Extension du panneau de configuration Windows
	SCR	Économiseur d'écran Windows
	VXD	Pilote de périphérique virtuel
	SYS	Pilote de périphérique système
	CLASS	Code binaire Java

	PYC	Script compilateur Python (code binaire)
	LIB	Bibliothèque de programme COFF (Common Object File Format)
	INS	Script InstallShield
	OBJ	Fichier objet
	O	Fichier objet
Archives compressées	ZIP	Archive compressée ZIP
	ARJ	Archive compressée ARJ
	RAR	Archive compressée WinRAR
	GZIP	Archive compressée GZIP
	TAR	Archive sur bande
	JAR	Archive compressée JAR
	ACE	Archive compressée WinAce
	HQX	Archive compressée Macintosh BinHex 4
	LZH	Archive compressée LHA
	LHA	Archive compressée LHA
	AR	Archive indexée AIX
	ARC	Archive compressée LH ARC
	CAB	Archive compressée Cabinet
	**_	Fichiers d'installation compressés (par exemple, EX_, DL_)
Images CD/DVD	ISO	Image disque ISO
	BIN	Image disque BIN
	CIF	Image disque EasyCD Creator
	CCD	Image disque CloneCD
	IMG	Image disque CloneCD
	MDF	Image disque Alcohol 120 %
	DAA	Image disque PowerISO
	C2D	Image disque WinOnCD
Bases de données	MDB	Base de données Microsoft Access
	ACCDB	Base de données Microsoft Access

	ACCDT	Modèle de base de données Microsoft Access
	MDA	Complément Microsoft Access
	MDW	Groupe de travail Microsoft Access
	MDE	Base de données compilée Microsoft Access
	MYD	Base de données MySQL MyISAM
	MYI	Index de base de données MySQL MyISAM
	FRM	Dictionnaire générique MySQL MyISAM
	DBF	Base de données dBase
	DBT	Base de données Microsoft FoxPro
	GDB	Base de données Borland InterBase
	PX	Base de données Paradox
Microsoft Outlook	PST	Dossiers personnels Outlook
	DBX	Dossier de messagerie Outlook Express
Chiffrement PGP	PGP	Chiffrement PGP (Pretty Good Privacy)
	ASC	Chiffrement sécurisé PGP (Pretty Good Privacy)
	CTX	Cryptogramme PGP (Pretty Good Privacy)
Conception Assistée par Ordinateur (CAO)	DWG	Dessin AutoCAD
	DXF	Échange de données AutoCAD
	ASM	Assemblage Pro/ENGINEER
	PRT	Modèle Pro/ENGINEER
Adobe FrameMaker	DOC	Document Adobe FrameMaker/FrameBuilder
	FM	Document Adobe FrameMaker
	FRM	Document Adobe FrameMaker
	BOOK	Livre Adobe FrameMaker
	MIF	Format d'échange de données Adobe FrameMaker

16.3.10 Étape 9 : Enregistrer et publier la stratégie

Les stratégies sont enregistrées et publiées comme décrit pour toutes les autres stratégies.

16.4 Listes blanches – Approbation de périphériques et de connexions WLAN

Les explications des sections suivantes concernent l'ajout de périphériques approuvés à la liste blanche *Contrôle du périphérique* et l'ajout de périphériques de stockage à la liste blanche *Contrôle du stockage*. Les différences entre l'ajout de périphériques de stockage et hors stockage sont mises en évidence et décrites.

Les explications sur l'ajout de réseaux WLAN approuvés sont disponibles dans *Ajout de connexions WLAN*.

SafeGuard Configuration Protection propose trois niveaux d'autorisations :

- **Types de périphériques et types de stockages :** cette option vous permet d'autoriser ou de restreindre l'accès à un point de terminaison en fonction du type de périphérique connecté. Par exemple : Supports amovibles, Adaptateurs réseau, Périphériques d'interface humaine (une souris par exemple) ou Périphériques d'imagerie. Les types de périphériques et les types de stockage pouvant être sélectionnés sont intégrés à SafeGuard Configuration Protection et accessibles dans les sections *Contrôle du périphérique* et *Contrôle du stockage*.
  Un type de périphérique peut être **autorisé** (par défaut), **bloqué** ou **restreint**. Si vous **restreignez** un type de périphérique, tous les périphériques de ce type sont bloqués sauf s'ils sont explicitement approuvés dans une liste blanche.

- **Liste blanche pour les modèles de périphériques :** cette option représente les modèles approuvés de périphériques ou de périphériques de stockage, toutes les imprimantes HP ou toutes les cartes mémoire USB M-Systems par exemple.

- **Liste blanche pour les périphériques distincts :** cette option fait référence à l'approbation de périphériques distincts ou de périphériques de stockage, chacun disposant d'un numéro de série unique, indiquant qu'il s'agit d'un périphérique spécifique.
  Par exemple, pour approuver l'utilisation de la carte mémoire USB du directeur général et bloquer toutes les autres cartes mémoire USB, vous devez définir le type de stockage Supports amovibles sur **Restreindre**, puis entrer les paramètres d'identification de la carte mémoire USB du directeur général dans une liste blanche de périphériques de stockage distincts spécifiques.

Cette section décrit comment

- créer une liste blanche ;

- ajouter des modèles approuvés ou des périphériques distincts à une liste blanche à partir de la liste de périphériques dont l'utilisation a été détectée dans votre organisation par SafeGuard PortAuditor ou manuellement.

16.4.1 Création de listes blanches

Pour enregistrer une liste blanche, procédez comme suit :

1. Sélectionnez **Liste blanche** dans la zone de navigation de stratégie.
2. Dans le menu contextuel de **Liste blanche**, cliquez sur **Nouveau** > **Liste blanche**.
3. Dans le champ **Nom de la liste blanche**, entrez le nom de la liste blanche.
4. **Sélection du type de liste blanche**

   Des listes blanches peuvent être créées pour :

   - Modèles de périphériques
   - Périphériques distincts
   - Modèles de périphériques de stockage
   - Périphériques de stockage distincts
   - Réseaux WLAN

   Les listes blanches individuelles peuvent être sélectionnées lors de la définition des paramètres de stratégie.
5. Spécifiez si vous souhaitez créer la liste blanche manuellement ou si vous envisagez d'utiliser le résultat d'une analyse des ordinateurs avec SafeGuard PortAuditor comme source.

Avis : les résultats de l'analyse SafeGuard PortAuditor doivent être disponibles (fichier XML) si vous envisagez de créer la liste blanche avec cette source.

a) **Créer manuellement une liste blanche**
Si vous sélectionnez cette option, une liste blanche vide s'ouvre dans SafeGuard Management Center après avoir cliqué sur **OK**. Vous pouvez créer manuellement des entrées dans cette liste blanche vide.

b) **Importer le résultat de SafeGuard® PortAuditor**
Si vous sélectionnez cette option, le résultat de l'analyse de SafeGuard PortAuditor est importé.

- Vous pouvez sélectionner le fichier fourni par SafeGuard PortAuditor via le bouton [**...**].
- Après avoir cliqué sur **OK**, le contenu du fichier importé s'affiche dans SafeGuard Management Center.

16.4.2 Ajout d'un périphérique à l'aide d'un fichier SafeGuard PortAuditor

Condition préalable : Création d'un fichier d'informations de périphérique

Pour créer un fichier contenant les informations relatives aux périphériques à approuver, utilisez SafeGuard PortAuditor pour analyser les ordinateurs requis. SafeGuard PortAuditor analyse les ordinateurs sélectionnés et signale tous les périphériques et réseaux WLAN actuellement ou précédemment connectés à ces ordinateurs. Les résultats d'audit sont enregistrés dans un fichier .XML. Pour en savoir plus sur SafeGuard PortAuditor, consultez le *manuel d'utilisation de SafeGuard PortAuditor 3.2*.

16.4.2.1 Étape 1 : Obtenir des informations sur le périphérique

Dans cette étape, vous spécifiez le fichier à partir duquel collecter les informations sur les périphériques à ajouter, à savoir l'emplacement du fichier .XML SafeGuard PortAuditor contenant les informations sur le périphérique requises. Une fois le fichier requis sélectionné à l'aide de [**...**], cliquez sur **OK** pour continuer.

16.4.2.2 Étape 2 : Sélectionner des périphériques

L'étape 2 affiche un tableau des périphériques détectés au niveau des points de terminaison de votre réseau et vous permet de sélectionner les périphériques à ajouter. Le tableau est divisé en catégories si la liste blanche à laquelle vous ajoutez des périphériques est une liste blanche de modèles de périphériques ou une liste blanche de périphériques distincts, et si vous ajoutez des périphériques de stockage ou hors stockage.

Les périphériques pouvant être sélectionnés disposent d'une case à cocher pour approuver le modèle de périphérique ou le périphérique distinct, le cas échéant. Vous pouvez également sélectionner ou désélectionner tous les périphériques ou les périphériques marqués en cliquant avec le bouton droit sur le tableau.

Avis : vous ne pouvez pas ajouter de périphériques de stockage à la liste blanche *Contrôle du périphérique*.

Avis : vous ne pouvez pas ajouter de périphériques ou de périphériques de stockage sans ID unique à une liste blanche de périphériques distincts.

Un périphérique peut parfois ne pas être identifié en tant que périphérique de stockage par SafeGuard PortAuditor. C'est le cas, par exemple, lorsqu'une classe de périphérique n'est pas intégrée par le fabricant. Si vous savez qu'il s'agit d'un périphérique de stockage, vous pouvez l'ajouter à la liste blanche de stockage de votre stratégie.

Vous ne devez pas ajouter de périphériques de stockage à une liste blanche *Contrôle du périphérique* ni ajouter de périphériques hors stockage à une liste blanche *Contrôle du stockage* car ils seront ignorés par le client SafeGuard Configuration Protection.

Avis : lorsque vous ajoutez un périphérique figurant déjà dans une autre liste blanche de périphériques de cette stratégie et que les autorisations de liste blanche sont différentes, les autorisations les plus strictes s'appliquent.

16.4.2.3 Étape 3 : Enregistrer une liste blanche

Enregistrez la liste blanche en cliquant sur l'icône de la barre d'outils de SafeGuard Enterprise.

Grâce au bouton **Modifier le contenu**, vous pouvez insérer le contenu d'un autre fichier dans la liste blanche.
Les nouvelles entrées sont ajoutées à la fin de la liste blanche.

16.4.3 Ajout manuel d'un périphérique

Si vous avez créé une liste blanche vide, vous devez ajouter les entrées manuellement.

Ou bien, pour ajouter des périphériques à une liste blanche existante, comme dans le cas de périphériques non connectés à un point de terminaison de votre organisation et n'apparaissant pas dans les résultats d'audit de SafeGuard PortAuditor, vous devez également les ajouter manuellement.

Les instructions suivantes s'appliquent à l'ajout de périphériques de stockage (*Contrôle du stockage*) et à l'ajout de périphériques hors stockage (*Contrôle du périphérique*).

Avis : lorsque vous ajoutez un périphérique figurant déjà dans une autre liste blanche de périphériques de cette stratégie et que les autorisations de liste blanche sont différentes, les autorisations les plus strictes s'appliquent.

Pour ajouter un périphérique manuellement :

1. Cliquez sur l'icône de la barre d'outils de SafeGuard Enterprise pour ajouter une nouvelle entrée à la liste blanche.
2. Entrez les informations demandées dans les champs suivants :
   a) **Port** (facultatif)
   b) **Description du périphérique** (facultatif)
   c) **Infos sur le périphérique** (facultatif)
   d) **Fournisseur (ID du fournisseur)** (facultatif)

e) **Produit (ID du produit)** (facultatif)

f) **ID du matériel / ID de l'instance** (**obligatoire**)

Vérifiez que vous avez entré les données correctes dans tous les champs et **enregistrez** la liste blanche.

Sélectionnez une entrée et cliquez sur l'icône de la barre d'outils de SafeGuard Enterprise pour supprimer l'entrée de la liste blanche.

Avis : l'ID du fournisseur (VID), l'ID du produit (PID), l'ID du matériel (HID) et l'ID de l'instance (IID) sont disponibles dans les résultats d'analyse de SafeGuard PortAuditor, sur une étiquette apposée sur le produit ou dans le gestionnaire de périphériques Windows.

16.4.4 Ajout de connexions WLAN

Les liens WLAN sont ajoutés à la liste blanche du *réseau local sans fil* quasiment de la même manière que les périphériques. Ajoutez une liste blanche WLAN, puis ajoutez des liens approuvés à cette liste blanche à l'aide des données du fichier SafeGuard Port Auditor ou manuellement.

16.4.4.1 Ajout manuel d'un lien WLAN

Pour ajouter des liens WLAN non détectés par SafeGuard PortAuditor et qui ne peuvent donc pas être ajoutés via le mécanisme d'importation, vous pouvez le faire manuellement.

Saisie d'informations sur le réseau local sans fil

Définissez les paramètres d'un réseau selon son ordre d'approbation de connexion.
Vous pouvez identifier un réseau par son nom et/ou son adresse MAC. Une fois le nom ou l'adresse MAC du réseau entré, vous pouvez également spécifier des paramètres d'authentification et de chiffrement de données à respecter. Seuls les réseaux répondant à tous les paramètres sont approuvés.

Pour ajouter un lien WLAN manuellement :

1. Ouvrez la liste blanche de connexions WLAN.
2. Cliquez sur l'icône de la barre d'outils de SafeGuard Enterprise pour ajouter une nouvelle entrée à la liste blanche.
3. Entrez un **Nom du réseau**, une **Adresse MAC** ou les deux. L'ajout d'informations à au moins un des deux champs est obligatoire.
4. Pour spécifier le **Nom du réseau** uniquement, entrez le nom et passez à l'étape 6.
5. Pour spécifier l'**Adresse MAC** uniquement, entrez l'adresse et passez à l'étape 6.

6. Pour définir des paramètres de sécurité, spécifiez les paramètres **Authentification** et **Chiffrement des données** requis dans la liste déroulante. L'ajout d'informations à ces champs est facultatif.

Avis : les options **Chiffrement des données** disponibles dans la liste déroulante dépendent du type d'**authentification** sélectionné. Par exemple, pour l'authentification WPA, les options de chiffrement sont TKIP ou AES alors que dans le cas de l'authentification 802.1X, seul le chiffrement WEP peut être sélectionné.

7. Vérifiez que vous avez entré les données correctes dans tous les champs et **enregistrez** la liste blanche.

16.5 Types de périphériques pris en charge

Ce chapitre répertorie les types de périphériques pouvant être sélectionnés pour SafeGuard Configuration Protection lors de la création d'une stratégie.

Pour les **périphériques hors stockage**, vous pouvez restreindre l'utilisation des périphériques sur les ports USB, FireWire et PCMCIA. SafeGuard Configuration Protection propose une sélection de types intégrés dans la fenêtre *Contrôle du périphérique* pour vous permettre de définir les types de périphériques approuvés ou bloqués. Si vous souhaitez contrôler un type de périphérique non répertorié, vous pouvez utiliser la fonction de restriction de périphérique distinct décrite dans *Listes blanches - Approbation de périphériques et de connexions WLAN*.

Pour les **périphériques de stockage**, SafeGuard PortAuditor peut généralement identifier un périphérique en tant que périphérique de stockage ou hors stockage en détectant son volume ou en utilisant ses données de classe intégrées. Cette fonction permet de classer et d'organiser des listes de périphériques en périphériques de stockage et en périphériques simples (hors stockage) à sélectionner, vous permettant ainsi de définir plus facilement votre stratégie. SafeGuard Configuration Protection propose une sélection de types intégrés dans la fenêtre *Contrôle du stockage* pour vous permettre de définir les types de périphériques approuvés ou bloqués.

Les listes de types de périphériques suivantes sont divisées en périphériques hors stockage et périphériques de stockage.

16.5.1 Types de périphériques hors stockage

La liste suivante répertorie les types de périphériques intégrés hors stockage pour lesquels une stratégie peut être définie dans SafeGuard Configuration Protection.

Avis : le contrôle du périphérique pour des périphériques hors stockage ne peut être défini que pour des ports USB, FireWire et PCMCIA.

1. **Périphériques d'interface humaine** : périphériques utilisés pour contrôler le fonctionnement des systèmes informatiques. Des exemples type incluent les claviers et dispositifs de pointage comme : une souris, une boule de commande et un manche.
2. **Périphériques d'impression** : imprimantes connectées via USB, PCMCIA ou FireWire.
3. **PDA (assistant numérique personnel)** : ils incluent :
   a) les périphériques Windows Mobile/Pocket PC ;
   b) les périphériques Blackberry ;
   c) les périphériques Palm OS.
4. **Téléphones mobiles** : nouveaux modèles de téléphones cellulaires, classés en tant que périphériques USB sans fil.
5. **Adaptateurs réseau** : périphériques de communication tels que : adaptateurs réseau Ethernet, adaptateurs réseau local sans fil (WLAN) et modems ADSL et câble connectés via USB.
6. **Périphériques d'imagerie** : principalement des périphériques comme des scanners et des appareils photo numériques.
7. **Périphériques audio/vidéo** : tels que : microphones, téléphones, commandes de volume, Webcams, caméscopes numériques, syntoniseurs de téléviseur numérique et appareils photo numériques prenant en charge la vidéotransmission en direct.
8. **Cartes à puce** : périphériques à carte à puce.
9. **Périphériques de sécurité de contenu** : utilisés pour proposer des fonctions de sécurité spécifiques, comme l'authentification stricte, l'identification biométrique et la gestion de licences.

16.5.2 Types de périphériques de stockage

La protection des périphériques de stockage s'applique à tous les ports non bloqués, à savoir aux périphériques de stockage spécifiés quel que soit le port auquel ils sont connectés tant que le port n'est pas défini comme étant bloqué.

Avis : le contrôle du périphérique des périphériques de stockage peut être défini pour tout type de port, par exemple, les ports parallèles, les ports USB, FireWire et PCMCIA.

La liste suivante répertorie les types de périphériques intégrés et pris en charge par SafeGuard Configuration Protection.

- **Périphériques de stockage amovibles** : ces périphériques incluent aussi bien des périphériques de stockage (cartes mémoire USB et cartes flash SD par exemple) que des périphériques à usage unique mais apparaissant sur l'ordinateur comme des nouveaux périphériques de stockage (lecteurs de musique numériques portables, appareils photo numériques et PDA par exemple).
- **Disques durs externes** : périphériques à disque dur reliés de manière externe (via USB par exemple).
- **Lecteurs de CD/DVD** : reliés de manière interne et externe.
- **Périphériques de disquette** : reliés de manière interne et externe.
- **Périphériques à bandes** : reliés de manière interne et externe.

17 Attribution utilisateur/ordinateur

SafeGuard Enterprise gère les informations concernant les utilisateurs autorisés à se connecter à une machine donnée figurant sur une liste nommée ci-dessous UMA (User Machine Assignment - Attribution utilisateur machine).

Pour qu'un utilisateur soit inclus à l'UMA, il doit s'être connecté une fois à un ordinateur sur lequel SafeGuard Enterprise a été installé et être enregistré dans SafeGuard Management Center en tant qu'utilisateur « complet » selon les termes de SafeGuard Enterprise. Un utilisateur « complet » désigne un utilisateur pour lequel un certificat a été généré après la première connexion et pour lequel un jeu de clés a été créé. Alors seulement les données de cet utilisateur peuvent être dupliquées sur d'autres ordinateurs. Après la duplication, l'utilisateur peut se connecter à cet ordinateur lors de l'authentification au démarrage.

Dans le paramètre standard, le premier utilisateur à se connecter à l'ordinateur après l'installation de SafeGuard Enterprise est saisi dans l'UMA en tant que propriétaire de cet ordinateur.

Cet attribut permet à l'utilisateur s'étant authentifié lors de l'authentification au démarrage, d'autoriser d'autres utilisateurs à se connecter à cet ordinateur. Ils seront également ajoutés à l'UMA pour cet ordinateur.

De ce fait, une liste automatique est générée et détermine quel utilisateur est autorisé à se connecter à quel ordinateur. Cette liste peut être modifiée dans SafeGuard Management Center.

17.1 Attribution utilisateur-ordinateur dans SafeGuard Management Center

Les utilisateurs peuvent être affectés à des ordinateurs spécifiques de SafeGuard Management Center. Si un utilisateur est affecté à un ordinateur dans SafeGuard Management Center (ou réciproquement) cette affectation est intégrée à l'UMA. Les données de l'utilisateur (certificat, clé, ...) sont dupliquées sur cet ordinateur et l'utilisateur peut s'y connecter.

Lors de la configuration de cette attribution, l'administrateur peut également spécifier qui peut autoriser d'autres utilisateurs à se connecter à cet ordinateur.

Dans **Type**, Management Center indique la méthode selon laquelle l'utilisateur a été ajouté à la base de données SafeGuard Enterprise. **Adopté** signifie que l'utilisateur a été ajouté à l'UMA d'un ordinateur final.

Avis : si personne n'est attribué dans Management Center et si aucun utilisateur n'est spécifié comme propriétaire, le premier utilisateur à se connecter à l'ordinateur après l'installation de SafeGuard Enterprise est saisi en tant que propriétaire. Cet utilisateur peut ensuite autoriser d'autres utilisateurs à se connecter à cet ordinateur.
Si des utilisateurs sont attribués à cet ordinateur dans Management Center à une date ultérieure, ils peuvent ensuite se connecter à l'authentification au démarrage. Néanmoins ces utilisateurs doivent être des utilisateurs complets (avec un certificat et une clé existants). Le propriétaire de l'ordinateur n'a pas besoin d'attribuer des droits d'accès dans ce cas.

Les paramètres suivants permettent de spécifier qui est autorisé à ajouter des utilisateurs à l'UMA :

- **Propriété :** Si ce paramètre est activé, l'utilisateur peut être enregistré comme le propriétaire d'un ordinateur.
- **Utilisateur propriétaire :** Ce paramètre signifie que l'utilisateur est saisi dans l'UMA en tant que propriétaire. Aucun utilisateur supplémentaire ne peut être inclus à l'UMA. Un seul utilisateur par ordinateur peut être saisi dans l'UMA en tant que propriétaire.

Le paramètre de stratégie **Importation de nouveaux utilisateurs autorisée pour** des **Paramètres machine spécifiques** détermine qui est autorisé à ajouter d'autres utilisateurs à l'UMA.

- **Importation de nouveaux utilisateurs autorisée pour**

  Personne
  Même l'utilisateur saisi comme propriétaire ne peut pas ajouter d'autres utilisateurs à l'UMA.
  L'option permettant à un propriétaire d'ajouter d'autres utilisateurs est désactivée.

  Propriétaire (paramètre par défaut)
  Les utilisateurs ne peuvent être ajoutés à l'UMA que par le propriétaire.

Avis : un responsable de la sécurité peut toujours ajouter des utilisateurs à SafeGuard Management Center.

Tout le monde

Lève la restriction selon laquelle les utilisateurs ne peuvent être ajoutés que par le propriétaire.

Exemple :

L'exemple suivant montre comment attribuer des droits de connexion dans SafeGuard Management Center à trois utilisateurs seulement (Utilisateur_a, Utilisateur_b, Utilisateur_c) pour Ordinateur_ABC.

Premièrement : Spécifiez la réponse dont vous avez besoin dans SafeGuard Enterprise Management Center. SafeGuard Enterprise est installé sur tous les ordinateurs finaux au cours de la nuit. Dans la matinée, les utilisateurs doivent se connecter à l'ordinateur conformément à leurs détails de connexion.

1. Dans SafeGuard Management Center, attribuez Utilisateur_a, Utilisateur_b et Utilisateur_c à Ordinateur_ABC. (Utilisateurs & ordinateurs -> Sélectionnez Ordinateur_ABC -> Attribuez l'utilisateur par Glisser-déposer). Vous avez ainsi spécifié un UMA.

2. Dans une stratégie d'ordinateur, définissez le paramètre Importation de nouveaux utilisateurs autorisée pour sur Personne. Puisque l'Utilisateur_a, l'Utilisateur_b et l'Utilisateur_c ne sont pas autorisés à ajouter de nouveaux utilisateurs, il n'est pas nécessaire de spécifier un utilisateur comme propriétaire.

3. Attribuez la stratégie à l'ordinateur et/ou à un point de la structure du répertoire auquel elle sera active pour l'ordinateur.

Lorsque le premier utilisateur se connecte à Ordinateur_ABC, une connexion automatique est mise en œuvre pour POA. Les stratégies de l'ordinateur sont envoyées à l'ordinateur final. Puisque l'Utilisateur_a est inclus dans l'UMA, il deviendra un utilisateur complet lors de sa connexion à Windows. Les stratégies de l'utilisateur, les certificats et les clés sont envoyés à l'ordinateur final. POA est activé.

Avis : l'utilisateur peut vérifier le message d'état dans l'icône de barre d'état de SafeGuard (infobulle) lorsque ce processus est terminé.

L'Utilisateur_a est à présent un utilisateur complet selon les termes de SafeGuard Enterprise et après la première connexion, il peut s'authentifier lors de l'authentification au démarrage et est connecté automatiquement.

L'Utilisateur_a quitte à présent l'ordinateur et l'Utilisateur_b souhaite se connecter. POA étant activé, il n'y a plus de connexion automatique.

L'Utilisateur_b et l'Utilisateur_c ont deux possibilités pour accéder à cet ordinateur.

a) L'Utilisateur_a désactive l'option Connexion automatique vers Windows dans la boîte de dialogue de connexion du POA et se connecte.

b) L'Utilisateur_b utilise la procédure challenge/réponse pour se connecter au POA.

Dans les deux cas, la boîte de dialogue de connexion de Windows s'affiche.

L'Utilisateur_b peut saisir ses informations d'identification Windows. Les stratégies de l'utilisateur, les certificats et les clés sont envoyés à l'ordinateur final. L'utilisateur est activé dans POA. L'Utilisateur_b est à présent un utilisateur complet selon les termes de SafeGuard Enterprise et après la première connexion, il peut s'authentifier lors de l'authentification au démarrage et sera connecté automatiquement.

Bien que la stratégie de l'ordinateur spécifie que personne ne peut importer d'utilisateurs dans cet ordinateur, du fait que ces utilisateurs se trouvent déjà dans l'UMA, l'Utilisateur_b et l'Utilisateur_c obtiennent néanmoins le statut d'utilisateur « complet » lors de la connexion à Windows et sont activés dans POA.

Aucun autre utilisateur ne sera ajouté à l'UMA ou ne pourra s'authentifier lors de l'authentification au démarrage. Les utilisateurs se connectant à Windows qui ne sont pas l'Utilisateur_a, l'Utilisateur_b ou l'Utilisateur_c sont exclus de l'UMA dans une telle situation et ne seront jamais actifs dans POA.

Les utilisateurs peuvent toujours être ajoutés par la suite à SafeGuard Management Center. Cependant, leur jeu de clés ne sera pas disponible après la première connexion, la synchronisation n'étant pas déclenchée par la première connexion. Après une deuxième connexion, le jeu de clés sera disponible et les utilisateurs pourront accéder à leur ordinateur selon les stratégies appliquées. S'ils n'ont jamais réussi à se connecter à un ordinateur final, il est possible de les ajouter comme indiqué ci-dessus.

Bloquer l'utilisateur

Si vous cochez la case dans la colonne **Bloquer l'utilisateur**, l'utilisateur n'est pas autorisé à se connecter à l'ordinateur concerné. De plus, l'ordinateur est arrêté automatiquement si l'utilisateur se connecte dès que la stratégie contenant ce paramètre est activée sur l'ordinateur.

17.1.1 Groupes

Des groupes d'ordinateurs peuvent également être attribués à un utilisateur (compte) et/ou des groupes peuvent être attribués à un ordinateur dans SafeGuard Management Center.

Exemple : Compte de service

C'est pourquoi il est par exemple possible d'utiliser un seul compte de service pour entretenir un grand nombre d'ordinateurs. À cette fin, les ordinateurs concernés doivent se trouver dans un même groupe. Ce groupe est ensuite attribué à un compte de service (utilisateur). Le propriétaire du compte de service peut ensuite se connecter à tous les ordinateurs de ce groupe.

En outre, le fait d'attribuer un groupe contenant différents utilisateurs permet à ces derniers de se connecter ensuite à un ordinateur spécifique en une seule étape.

17.2 Attribution de groupes d'utilisateurs et d'ordinateurs

Pour attribuer un utilisateur à un groupe d'ordinateurs, procédez de la façon suivante :

Avis : vous pouvez attribuer des utilisateurs individuels à un ordinateur ou réciproquement en utilisant la même procédure que pour les groupes.

1. Cliquez sur **Utilisateurs & ordinateurs**.
2. Pour attribuer un groupe d'ordinateurs à un utilisateur unique, sélectionnez ce dernier.
3. Cliquez sur l'onglet **Ordinateur** dans la zone d'action.

   Tous les ordinateurs et groupes d'ordinateurs sont affichés sous Ordinateurs disponibles.
4. Faites glisser les groupes sélectionnés de la liste des groupes disponibles jusqu'à la zone d'activation.
5. Une boîte de dialogue s'affiche demandant si l'utilisateur doit être le propriétaire de tous les ordinateurs.

   Si aucun propriétaire n'est spécifié dans SafeGuard Enterprise Management, le premier utilisateur à se connecter à cet ordinateur en devient automatiquement le propriétaire. Cet utilisateur peut autoriser d'autres utilisateurs à accéder à cet ordinateur. La condition est que l'utilisateur soit défini sur « Can be owner (Peut être propriétaire) ».

- Le fait de répondre **Oui** à cette question signifie que le premier utilisateur à se connecter à cet ordinateur en devient le propriétaire et peut en autoriser l'accès à d'autres utilisateurs.
- Le fait de répondre **Non** à cette question signifie que l'utilisateur ne sera pas le propriétaire de cet ordinateur.

  Il n'est généralement pas nécessaire pour le propriétaire d'un compte de service d'être en même temps le propriétaire de l'ordinateur. Ce paramètre peut être modifié après l'attribution initiale.

6. Après avoir répondu à la question, tous les ordinateurs du groupe attribué sont affichés dans la zone d'action.

L'utilisateur peut se connecter à tous les ordinateurs attribués de cette manière.

Un groupe d'utilisateurs peut être attribué à un seul ordinateur en utilisant la même procédure.

18 Clés cryptographiques et cartes à puce

Les clés cryptographiques et les cartes à puce sont des composants matériels qui aident un utilisateur autorisé dans la procédure d'authentification sur un système informatique. Elles permettent de stocker des certificats, des signatures numériques et des informations biométriques. Ces données ne peuvent pas être manipulées.

De nos jours, il est fréquent que l'authentification utilisant un nom d'utilisateur et un mot de passe ne réponde plus aux besoins des clients qui souhaitent bénéficier de la meilleure protection possible contre les accès externes. Alternative destinée à améliorer la sécurité, SafeGuard Enterprise permet de se connecter en utilisant des clés cryptographiques et des cartes à puce. La connexion par clé cryptographique est basée sur le principe d'une authentification en deux étapes : l'utilisateur possède une clé cryptographique (propriété), mais il ne peut l'utiliser que s'il en connaît le mot de passe (connaissance). Lorsqu'une clé cryptographique ou une carte à puce sont utilisées, leur présence et un code PIN suffisent à l'utilisateur pour s'authentifier.

Avis : les cartes à puce et les clés cryptographiques sont traitées de la même manière dans SafeGuard Enterprise. Les termes « clé cryptographique » et « carte à puce » recouvrent la même notion dans le produit et le manuel.

Les clés cryptographiques sont prises en charge :

- dans l'authentification au démarrage ;
- au niveau du système d'exploitation ;
- pour se connecter à Management Center.

Lorsqu'une clé cryptographique est générée pour un utilisateur, des informations telles que le fabricant, le type, le numéro de série, les données de connexion et les certificats sont stockées dans la base de données SafeGuard Enterprise. Dans de telles situations, les clés cryptographiques sont identifiées par un numéro de série, puis reconnues dans SafeGuard Enterprise.

Ceci confère des avantages non négligeables :

- L'identification des clés cryptographiques en circulation et des utilisateurs auxquels elles sont attribuées est aisée.
- Leur date et heure de génération sont également connues.
- En cas de perte d'une clé cryptographique, le responsable de la sécurité est en mesure de l'identifier et de la bloquer en vue de son authentification. Ces mesures évitent toute utilisation frauduleuse de données.
- Toutefois, le responsable de la sécurité peut utiliser la procédure Challenge/Réponse pour autoriser temporairement la connexion sans clé cryptographique, par exemple si un utilisateur a oublié son code PIN.

18.1 Cartes à puce

Pour pouvoir utiliser une carte à puce avec SafeGuard Enterprise, un lecteur de cartes et un pilote de carte pour le PC sont nécessaires en plus de la carte à puce elle-même. En outre, pour que les cartes à puce et les lecteurs de carte puissent communiquer avec SafeGuard Enterprise, certains composants middleware, sous la forme d'un module PKCS#11, sont nécessaires.

18.1.1 Cartes à puce et lecteurs/pilotes de cartes à puce

SafeGuard Enterprise prend en charge les procédures de connexion non cryptographiques et cryptographiques avec l'authentification au démarrage. Avec les cartes à puce non cryptographiques, l'ID utilisateur et le mot de passe sont stockés sur la carte. Les cartes à puce cryptographiques sont utilisées pour authentifier les paires de clés RSA (certificats).

Windows

- Dans le système d'exploitation Windows, les lecteurs de cartes compatibles PC/SC sont pris en charge. L'interface PC/SC régit la communication entre le PC et la carte à puce. Nombre de ces lecteurs de cartes sont déjà intégrés dans l'installation de Windows.
- Les cartes à puce requièrent des pilotes compatibles PKCS#11 si elles doivent être prises en charge par SafeGuard Enterprise.

Authentification au démarrage

Reportez-vous aux Notes de version pour obtenir une liste détaillée de toutes les cartes à puce, lecteurs de cartes à puce et pilotes de cartes à puce pris en charge.

- Avec l'authentification au démarrage, c'est l'interface PC/SC qui régit la communication entre le PC et la carte à puce. Les pilotes de cartes à puce pris en charge sont fixés, de sorte que les utilisateurs ne peuvent pas en ajouter. Les pilotes de cartes à puce appropriés doivent être activés au moyen d'une stratégie dans SafeGuard Enterprise.
- L'interface des lecteurs de cartes à puce est standardisée et un grand nombre de ces lecteurs possèdent une interface USB ou une interface ExpressCard/54 et mettent en œuvre la norme CCID. Dans SafeGuard Enterprise, il s'agit d'une condition préalable à la prise en charge avec l'authentification au démarrage. De plus, du côté du pilote, le module PKCS#11 doit être pris en charge.

18.1.2 Cartes à puce prises en charge avec l'authentification au démarrage

SafeGuard Enterprise prend en charge un grand nombre de cartes à puce et de lecteurs de cartes à puce, ainsi que les pilotes de cartes à puce courants avec l'authentification au démarrage. Avec SafeGuard Enterprise, les clés cryptographiques/cartes à puce compatibles avec les opérations 2 048 bits RSA sont prises en charge. La prise en charge des cartes à puce faisant l'objet d'améliorations d'une version à la suivante, les clés cryptographiques et cartes à puce pour la version actuelle de SafeGuard Enterprise sont répertoriés dans les Notes de version.

18.1.3 Middleware pris en charge

Le middleware de la liste ci-dessous est pris en charge via le module PKCS#11 correspondant. PKCS#11 est une interface standardisée pour connecter des clés cryptographiques/cartes à puce à différents logiciels. Elle est utilisée ici pour la communication entre la clé cryptographique/carte à puce, le lecteur de carte à puce et SafeGuard Enterprise.

Fabricant	Middleware
ActivIdentity	ActivClient
Aladdin	eToken PKI Client
AET	SafeSign Identity Client
Charismatics	Smart Security Interface
RSA	RSA Authentication Client 2.x RSA Smart Card Middleware 3.x
Siemens	CardOS API
A-Trust	a.sign Client
Gemalto	Gemalto .NET Card Gemalto Classic Client Gemalto Access Client
Solution informatique GmbH	IT Solution trustWare CSP+
Sertifitseerimiskeskus AS	Estonian ID Card
T-Systems	NetKey 3.0

Informations de licence pour Siemens et Charismatics :

Sachez que l'utilisation du middleware respectif pour le système d'exploitation standard requiert un contrat de licence avec Siemens Medical/Charismatics. Pour obtenir des licences, renseignez-vous à l'adresse suivante :

- Global Siemens Healthcare Headquarters
  Siemens AG
  Healthcare Sector
  Henkestrasse 127
  D-91052 Erlangen
  Allemagne
  Tél.: +49 69 797 6602

- *http://www.charismathics.com/cryptoshop/shop_content.php*
  ou à l'adresse
  sales@charismathics.com

Le middleware est défini à l'aide d'une stratégie dans SafeGuard Enterprise. Le package de configuration du client SafeGuard Enterprise doit également être installé sur le PC sur lequel Management Center est exécuté.

18.2 Clés cryptographiques USB

De même que les cartes à puce, les clés cryptographiques USB comportent un lecteur de cartes à puce et une carte à puce, ces deux unités se trouvant dans un même boîtier.

18.2.1 Clés cryptographiques prises en charge avec l'authentification au démarrage

SafeGuard Enterprise prend en charge une vaste gamme de clés cryptographiques USB. Comme condition préalable, la carte à puce utilisée doit être prise en charge par l'authentification au démarrage de SafeGuard Enterprise et les lecteurs correspondants doivent également être pris en charge. Les clés cryptographiques USB doivent également être prises en charge par le middleware correspondant.

La prise en charge des clés cryptographiques faisant l'objet d'améliorations d'une version à la suivante, les clés cryptographiques et cartes à puce pour chaque version de SafeGuard Enterprise sont répertoriées dans les Notes de version.

18.3 Utilisation des clés cryptographiques

Pour pouvoir utiliser des clés cryptographiques pour l'authentification, procédez comme suit :

1. Initialiser des clés cryptographiques vides.
2. Générer des clés cryptographiques pour les responsables de la sécurité.
3. Écrire les certificats et les clés sur les clés cryptographiques.
4. Définir des stratégies pour les clés cryptographiques.

Vous pouvez également utiliser des clés cryptographiques dont les données proviennent d'une application différente pour l'authentification à condition qu'elles disposent de suffisamment d'espace de stockage pour les certificats et les informations de connexion.

SafeGuard Enterprise vous offre les fonctions suivantes afin que vous puissiez facilement administrer les clés cryptographiques :

- affichage et filtrage des informations de la clé cryptographique ;
- initialisation, modification, réinitialisation et blocage des codes PIN ;
- lecture et suppression des données de la clé cryptographique ;
- blocage de la clé cryptographique.

18.4 Initialisation d'une clé cryptographique

Avant qu'une clé cryptographique « vide », non formatée puisse être générée pour un utilisateur de SafeGuard Enterprise, elle doit être préparée pour l'utilisation, c'est-à-dire initialisée, conformément aux instructions fournies par son fabricant. Lorsqu'elle est initialisée, des informations de base, par exemple le code PIN standard, sont écrites sur cette clé. Le logiciel d'initialisation du fabricant de la clé cryptographique permet de réaliser cela.

Veuillez consulter le fabricant de la clé cryptographique pour obtenir davantage d'informations.

18.4.1 Installation du middleware sur l'ordinateur final

Installez ensuite le middleware approprié, à la fois sur le PC sur lequel SafeGuard Management Center est exécuté et sur le PC d'utilisateur concerné. Pour cela, voir *Middleware pris en charge* en page 191.

18.4.2 Activation du middleware (module PKCS#11)

Avant de générer la clé cryptographique, vous devez attribuer le middleware approprié sous la forme du module PKCS#11 en définissant une stratégie dans SafeGuard Management Center. Vous devez le faire à la fois sur le PC sur lequel SafeGuard Management Center est exécuté et sur le PC d'utilisateur. C'est la condition nécessaire pour que SafeGuard Enterprise communique avec la clé cryptographique. Vous pouvez définir le paramètre du module PKCS#11 en utilisant une stratégie, de la façon suivante.

Condition préalable : le middleware est installé sur le PC concerné et la clé cryptographique a été initialisée. Le package de configuration du client SafeGuard Enterprise doit également être installé sur le PC sur lequel Management Center est exécuté.

Dans SafeGuard Management Center, cliquez sur **Stratégies**.

1. Connectez la clé cryptographique à l'interface USB. SafeGuard Enterprise lit la clé cryptographique.
2. Créez une nouvelle stratégie du type **Paramètres machine spécifiques** ou sélectionnez une stratégie existante de ce type.
3. Dans la zone de travail du côté droit, sous **Paramètres de support de carte à puce** > **Nom du module**, sélectionnez le middleware approprié. Enregistrez les paramètres.
4. Attribuez la stratégie.

À présent, SafeGuard Enterprise peut communiquer avec la clé cryptographique et l'administrer. La clé cryptographique peut maintenant être générée.

18.5 Génération d'une clé cryptographique

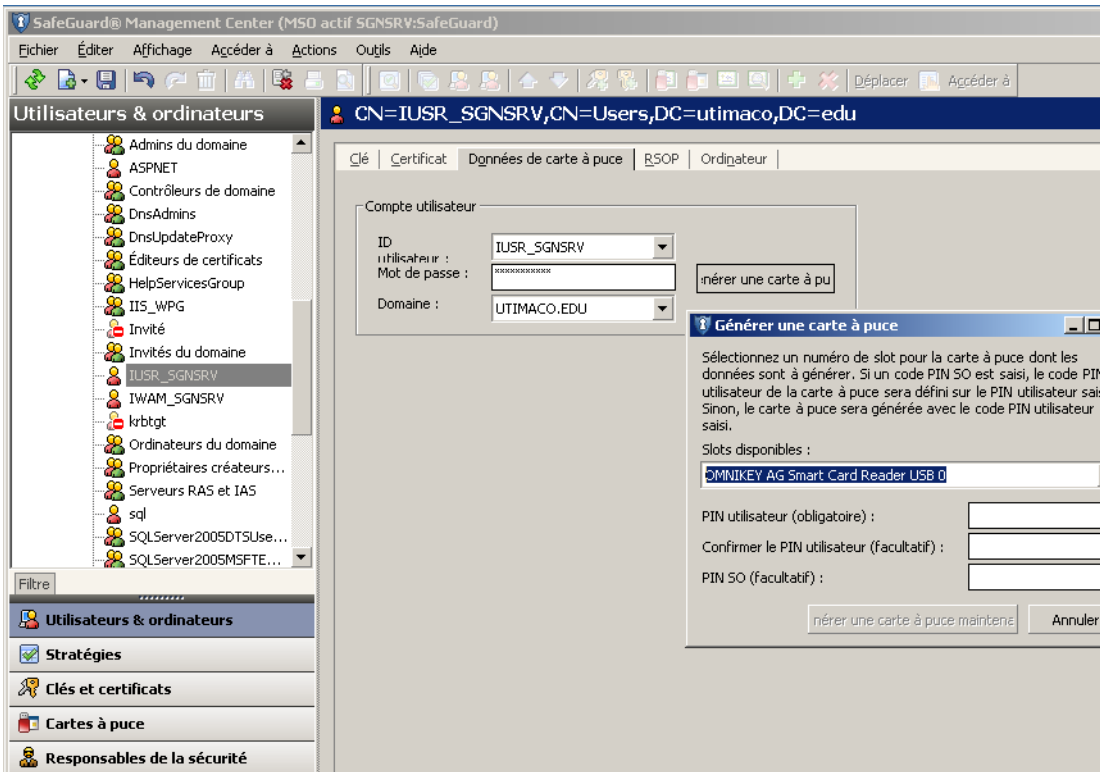
Lorsqu'une clé cryptographique est générée dans SafeGuard Enterprise, les données sont écrites sur cette clé cryptographique qui est ensuite utilisée pour l'authentification. Ces données sont constituées d'informations d'identification et de certificats.

Dans SafeGuard Enterprise, des clés cryptographiques peuvent être générées pour les rôles d'utilisateurs suivants :

- clés cryptographiques pour les utilisateurs classiques ;
- clés cryptographiques pour les responsables de la sécurité (SO).

L'utilisateur et le responsable de la sécurité (SO) peuvent accéder à la clé cryptographique. L'utilisateur est la personne qui doit utiliser la clé cryptographique. L'utilisateur n'a accès qu'aux objets et aux clés privés. Le SO ne peut accéder qu'aux objets publics, mais il peut réinitialiser le code PIN de l'utilisateur.

18.5.1 Génération d'une clé cryptographique ou d'une carte à puce pour un utilisateur



Condition préalable : la clé cryptographique doit être initialisée et le module PKCS#11 approprié doit être activé.
Le package de configuration du client SafeGuard Enterprise doit également être installé sur le PC sur lequel Management Center est exécuté.

Ouvrez Management Center et cliquez sur **Utilisateurs & ordinateurs**.

1. Connectez la clé cryptographique à l'interface USB. SafeGuard Enterprise lit la clé cryptographique.
2. Cochez l'utilisateur pour lequel une clé cryptographique doit être générée, et ouvrez l'onglet **Données de la carte à puce** dans la zone de travail du côté droit.
3. Dans la boîte de dialogue **Données de la carte à puce**, procédez comme suit :
   a) Sélectionnez l'ID utilisateur et le domaine de l'utilisateur sélectionné et entrez votre mot de passe Windows.
   b) Cliquez sur **Générer une carte à puce**.
4. Dans la boîte de dialogue **Générer une carte à puce**, sélectionnez le slot approprié pour la clé cryptographique.
5. Générez un nouveau **PIN utilisateur** et répétez la saisie.
6. Sous **PIN SO**, entrez le PUK standard fourni par le fabricant ou le code PIN généré lorsque la clé cryptographique a été initialisée.

Avis : si vous remplissez uniquement le champ **PIN utilisateur (obligatoire)**, le code PIN de l'utilisateur doit correspondre à celui qui a été généré lors de l'initialisation de la clé cryptographique. Il est alors inutile de répéter le code PIN de l'utilisateur ou de saisir un code PIN SO.

7. Cliquez sur **Générer une carte à puce maintenant**.

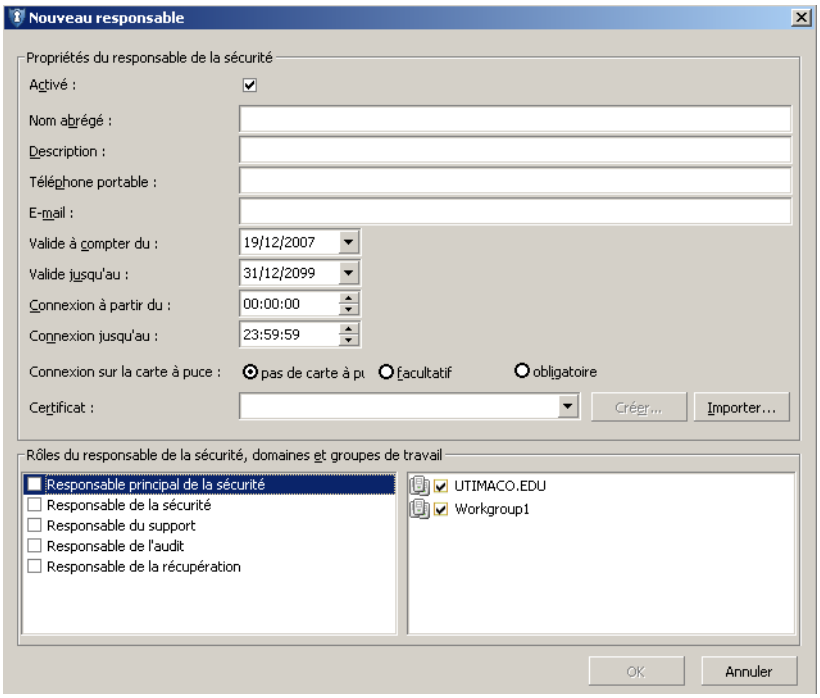
La clé cryptographique est générée, les informations de connexion écrites sur la clé cryptographique et les informations de la clé cryptographique enregistrées dans la base de données SafeGuard Enterprise. Vous pouvez afficher les données de la zone **Carte à puce** de l'onglet **Informations sur la carte à puce**.

18.5.2 Génération d'une clé cryptographique ou d'une carte à puce pour un responsable de la sécurité

Lorsque SafeGuard Enterprise est installé la première fois, le premier responsable de la sécurité (SO) a la possibilité de générer pour lui-même une clé cryptographique et de spécifier le mode de connexion (consultez le Guide d'installation). Pour tous les autres responsables de la sécurité, une clé cryptographique est générée dans SafeGuard Enterprise Management Center.

Condition préalable : la clé cryptographique doit être initialisée et le module PKCS#11 approprié doit être activé. Vous devez disposer des droits nécessaires pour effectuer des sélections pour le SO.

Dans SafeGuard Management Center, cliquez sur **Responsables de la sécurité**.



1. Connectez la clé cryptographique à l'interface USB. SafeGuard Enterprise lit la clé cryptographique.
2. Dans la fenêtre de navigation de gauche, cochez **Responsable de la sécurité** et dans le menu contextuel, sélectionnez **Nouveau** > **Nouveau responsable**.
3. Si le SO doit s'authentifier avec ou sans clé cryptographique, dans la zone de travail du côté droit, activez **Connexion sur la carte à puce : facultatif**.

4. Si le SO ne doit s'authentifier qu'avec la clé cryptographique, activez **Connexion sur la carte à puce : obligatoire**. Avec ce paramètre, la clé privée reste sur la clé cryptographique. La clé cryptographique doit toujours être connectée, sinon, le système doit être réinitialisé.
5. Si vous souhaitez créer un certificat, cliquez sur **Créer**. Entrez deux fois le mot de passe du certificat et confirmez en cliquant sur **OK**. Indiquez l'emplacement d'enregistrement du certificat.
6. Si vous souhaitez importer des certificats, cliquez sur **Importer**. Ouvrez le fichier de certificat concerné. La recherche s'effectue d'abord dans un fichier de certificat, puis sur la clé cryptographique. Les certificats peuvent rester dans l'emplacement de stockage quel qu'il soit.
7. Activez les rôles et les domaines devant être attribués au SO.
8. Confirmez les saisies en cliquant sur **OK**.

Le SO est créé, la clé cryptographique est générée, les informations de connexion sont, selon le paramètre, écrites sur la clé cryptographique et les informations de la clé cryptographique sont enregistrées dans la base de données SafeGuard Enterprise. Vous pouvez afficher les données de la zone **Carte à puce** de l'onglet **Informations sur la carte à puce**.

18.6 Placement des certificats sur une clé cryptographique ou sur une carte à puce

Les informations de connexion, mais également les certificats peuvent être écrits sur une clé cryptographique. Seule la partie privée du certificat (fichier .p12) peut être enregistrée sur la clé cryptographique. Toutefois, les utilisateurs ne peuvent normalement accéder qu'à leur clé privée lorsqu'ils se connectent avec la clé cryptographique. Il est recommandé d'utiliser des certificats d'une infrastructure de clé publique (PKI).

Vous pouvez attribuer les données d'authentification à différents types de clés cryptographiques :

- en générant des certificats directement sur la clé cryptographique ;
- en attribuant des données qui se trouvent déjà sur la clé cryptographique ;
- en important des certificats d'un fichier.

Avis : les certificats de l'AC ne peuvent pas provenir d'une clé cryptographique et être stockés dans la base de données ou dans le magasin de certificats. Si vous souhaitez (ou si vous avez besoin) d'utiliser des certificats de l'AC, ces derniers doivent être disponibles sous forme de fichier et pas seulement sous forme de clé cryptographique. Ceci s'applique également aux CRL (liste de révocation des certificats).
De surcroît, les certificats de l'AC doivent correspondre à la CRL de la clé cryptographique, sinon les utilisateurs ne peuvent pas se connecter aux ordinateurs concernés. Vérifiez que l'AC et la CRL sont correctes. SafeGuard Enterprise n'effectue pas cette vérification.
SafeGuard Enterprise ne peut ensuite communiquer avec les certificats ayant expiré que si les clés nouvelles et anciennes sont présentes sur la même carte.

18.6.1 Génération de certificats avec des clés cryptographiques

Vous pouvez générer de nouveaux certificats directement à partir de la clé cryptographique si, par exemple, aucune structure de certificat n'est présente.

Avis : si seule la partie privée du certificat est écrite sur la clé cryptographique, cette dernière permet à l'utilisateur d'accéder uniquement à sa clé privée. La clé privée ne se trouve alors que sur la clé cryptographique. En cas de perte de la clé cryptographique, la clé privée devient inaccessible.

Condition préalable : la clé cryptographique a été générée.

Dans SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs**.

1. Connectez la clé cryptographique à l'interface USB. SafeGuard Enterprise lit la clé cryptographique.
2. Cochez l'utilisateur pour lequel un certificat doit être généré, et ouvrez l'onglet **Certificat** dans la zone de travail du côté droit.
3. Cliquez sur **Générer et attribuer un certificat par carte à puce**. Notez que la longueur de la clé doit correspondre à la taille de la clé cryptographique.
4. Sélectionnez le slot et saisissez le code PIN de la clé cryptographique. Cliquez sur **Créer**.

La clé cryptographique génère le certificat et l'attribue à l'utilisateur.

18.6.2 Attribution de certificats de clé cryptographique à un utilisateur

S'il existe déjà des certificats sur la clé cryptographique que vous voulez attribuer à l'utilisateur, procédez de la façon suivante :

Condition préalable : la clé cryptographique a été générée.

Dans SafeGuard Management Center, cliquez sur **Utilisateurs & ordinateurs**.

1. Connectez la clé cryptographique à l'interface USB. SafeGuard Enterprise lit la clé cryptographique.
2. Cochez l'utilisateur pour lequel vous voulez attribuer un certificat, et ouvrez l'onglet **Certificat** dans la zone de travail du côté droit.
3. Cliquez sur l'icône **Attribuer un certificat à partir d'une carte à puce** de la barre d'outils de SafeGuard Management Center. Sélectionnez le certificat concerné dans la liste et saisissez le code PIN de la clé cryptographique.
4. Confirmez en cliquant sur **OK**.

Le certificat est attribué à un l'utilisateur.

18.6.3 Placement d'un certificat depuis un fichier sur la clé cryptographique

Si vous voulez ajouter la partie privée du certificat (fichier .p12 file) depuis un fichier sur la clé cryptographique, procédez de la façon suivante :

Condition préalable : la clé cryptographique a été générée.

Dans SafeGuard Management Center, cliquez sur **Cartes à puce**.

1. Connectez la clé cryptographique à l'interface USB. SafeGuard Enterprise lit la clé cryptographique.
2. Cochez la clé cryptographique à laquelle vous voulez ajouter la partie privée du certificat et ouvrez l'onglet **Informations d'identification & Certificats** dans la zone de travail du côté droit.
3. Cliquez sur l'icône **P12 à carte à puce** de la barre d'outils de SafeGuard Management Center. Sélectionnez le fichier de certificat concerné.
4. Entrez le code PIN de la clé cryptographique et le mot de passe du fichier .p12 et confirmez en cliquant sur **OK**.

La partie privée du certificat est ajoutée à la clé cryptographique. À présent, vous devez l'ajouter à un utilisateur. Pour cela, voir *Attribution de certificats de clé cryptographique à un utilisateur* en page 200.

Avis : pour une clé cryptographique avec support Kerberos, vous devez sélectionner cette procédure. Le certificat doit être reconnu par SafeGuard Enterprise et ajouté à la clé cryptographique. S'il existe déjà un certificat généré automatiquement, le certificat importé le remplacera.

18.7 Attribution de stratégies pour les clés cryptographiques

Lorsque vous attribuez des stratégies, vous pouvez spécifier d'autres options de clé cryptographique. Elles concernent :

- les codes PIN ;
- le mode de connexion ;
- la définition de codes PIN de clés cryptographiques pour la connexion automatique à l'authentification au démarrage ;
- ce qui se produit lorsque l'état de la clé cryptographique n'est plus reconnu ;
- le déblocage de la clé cryptographique ;
- le middleware à utiliser (module PKCS#11).

18.8 Utilisation de clés cryptographiques pour se connecter à l'authentification au démarrage

Pour se connecter à partir de l'authentification au démarrage avec une clé cryptographique, procédez comme suit :

Condition préalable : notez que le support USB est activé dans le BIOS. Le support de clé cryptographique doit être initialisé et la clé cryptographique doit être générée.

1. Connectez la clé cryptographique à l'interface USB.
2. Mettez le PC sous tension et attendez l'arrêt de l'authentification au démarrage.
3. Entrez le code PIN de la clé cryptographique.

Vous êtes connecté à SafeGuard Enterprise.

Mode de connexion à l'authentification au démarrage

Il existe deux méthodes de connexion à l'aide d'une clé cryptographique. Il est possible de combiner les deux méthodes de connexion.

- Connexion avec ID utilisateur/mot de passe
- Connexion avec clé cryptographique

  Lorsque vous vous connectez avec une clé cryptographique/carte à puce, vous pouvez sélectionner la méthode non cryptographique ou la méthode Kerberos (cryptographique). Les procédures Challenge/Réponse sont impossibles avec Kerberos car aucune information de connexion n'est disponible dans l'authentification au démarrage.

Le responsable de la sécurité spécifie la méthode à utiliser pour les utilisateurs et les ordinateurs dans une stratégie du type Authentification.

18.9 Activation de la connexion automatique à l'authentification au démarrage avec des codes PIN de clés cryptographiques par défaut

Grâce à un code PIN de clé cryptographique par défaut distribué dans une stratégie, une connexion utilisateur automatique peut être possible lors de l'authentification au démarrage. Ceci permet de ne pas générer chaque clé cryptographique séparément et permet aux utilisateurs de se connecter automatiquement lors de l'authentification au démarrage sans action de l'utilisateur.

Lorsqu'une clé cryptographique est utilisée lors de la connexion et qu'un code PIN par défaut est attribué à l'ordinateur, l'utilisateur est connecté automatiquement à l'authentification au démarrage sans qu'il ait besoin de saisir un code PIN.

En tant que responsable de la sécurité, vous pouvez définir le code PIN spécifique dans une stratégie du type **Authentification** et l'attribuer à différents ordinateurs ou groupes d'ordinateurs, par exemple à tous les ordinateurs d'un même lieu.

Pour activer la connexion automatique avec un code PIN de clé cryptographique par défaut, procédez comme suit :

1. Dans SafeGuard Management Center, cliquez sur **Stratégies**.
2. Sélectionnez une stratégie du type **Authentification**.
3. Sous **Options de connexion**, dans **Mode de connexion**, sélectionnez **Carte à puce**.
4. Dans **Code PIN utilisé pour la connexion automatique avec une carte à puce**, spécifiez le code PIN par défaut à utiliser pour la connexion automatique. Dans ce cas, il n'est pas nécessaire de suivre les règles relatives au code PIN.

Avis : ce paramètre n'est disponible que si vous sélectionnez **Carte à puce** comme **mode de connexion** possible.

5. Dans **Authentification automatique à Windows**, définissez **Désactiver l'authentification automatique à Windows**. Si vous ne sélectionnez pas cette option lorsqu'un code PIN par défaut est spécifié, vous ne pourrez pas enregistrer la stratégie.

   Si vous souhaitez activer l'option **Authentification automatique à Windows**, vous pouvez créer ultérieurement une autre stratégie du type **Authentification** dans laquelle cette option est activée, et l'attribuer au même groupe d'ordinateurs afin que les deux stratégies soient actives dans le RSOP.

6. Vous pouvez également spécifier d'autres paramètres de clé cryptographique.
7. Enregistrez vos paramètres et attribuez la stratégie aux ordinateurs ou groupes d'ordinateurs concernés.

Windows démarre si la connexion automatique sur l'ordinateur final réussit.

En cas d'échec de la connexion automatique sur l'ordinateur final, l'utilisateur est invité à entrer le code PIN de clé cryptographique lors de l'authentification au démarrage.

18.10 Initialisation, changement et blocage des codes PIN

Si vous êtes un responsable de la sécurité, vous pouvez changer le code PIN de l'utilisateur et celui du SO, de même que vous pouvez également forcer le changement du code PIN de l'utilisateur. Ceci est généralement nécessaire lors de la génération d'une clé cryptographique. Vous pouvez également initialiser des codes PIN, c'est-à-dire les générer comme de nouveaux codes PIN, et les bloquer.

Vous pouvez utiliser des stratégies pour spécifier d'autres options de code PIN pour l'ordinateur final.

Avis : notez que lorsque vous changez un code PIN, certains fabricants de clés cryptographiques spécifient leurs propres règles de code PIN qui peuvent contredire celles de SafeGuard Enterprise. C'est la raison pour laquelle il se peut qu'il ne soit pas possible de changer un code PIN comme vous le souhaitez, même s'il respecte les règles des codes PIN de SafeGuard Enterprise. C'est pourquoi vous devez toujours consulter les règles des codes PIN du fabricant de la clé cryptographique. Elles peuvent être affichées dans la zone **Carte à puce** sous **Informations sur la carte à puce** dans Management Center.

Les codes PIN sont gérés dans Management Center sous **Cartes à puce**. La clé cryptographique est connectée et cochée dans la fenêtre de navigation de gauche.

18.10.1 Initialisation du code PIN utilisateur

Condition préalable : le code PIN du SO doit être connu.

1. Pour générer de nouveau le code PIN de l'utilisateur, cliquez sur l'icône **Initialiser le PIN utilisateur**. Saisissez le code PIN du SO.
2. Saisissez le nouveau code PIN de l'utilisateur, répétez la saisie et confirmez en cliquant sur **OK**.

Le code PIN de l'utilisateur est initialisé.

18.10.2 Changement d'un code PIN SO

Condition préalable : le code PIN du SO précédent doit être connu.

1. Pour changer le code PIN du SO, cliquez sur l'icône **Changer le PIN SO** de la barre d'outils de SafeGuard Management Center.
2. Saisissez l'ancien code PIN du SO.
3. Saisissez le nouveau code PIN du SO, répétez la saisie et confirmez en cliquant sur **OK**.

Le code PIN du SO est initialisé.

18.10.3 Changement d'un code PIN utilisateur

Condition préalable : le code PIN de l'utilisateur doit être connu.

1. Pour changer le code PIN de l'utilisateur, cliquez sur l'icône **Changer le PIN utilisateur** de la barre d'outils de SafeGuard Management Center.
2. Saisissez l'ancien et le nouveau code PIN de l'utilisateur, répétez la saisie du nouveau code PIN de l'utilisateur et confirmez en cliquant sur **OK**.

Le code PIN de l'utilisateur est initialisé. Si vous avez changé le code PIN d'un autre utilisateur, informez-le de cette modification.

18.10.4 Changement de code PIN forcé

Pour forcer le changement de code PIN, procédez comme suit :

1. Cliquez sur l'icône **Forcer le changement de PIN** de la barre d'outils de SafeGuard Management Center.

Lors de la prochaine connexion de l'utilisateur avec la clé cryptographique, il doit changer son code PIN.

18.10.5 Historique des codes PIN

L'historique des codes PIN peut être supprimé. Pour cela, cliquez sur l'icône **Supprimer l'historique de PIN** de la barre d'outils de SafeGuard Management Center.

18.11 Gestion des clés cryptographiques et des cartes à puce

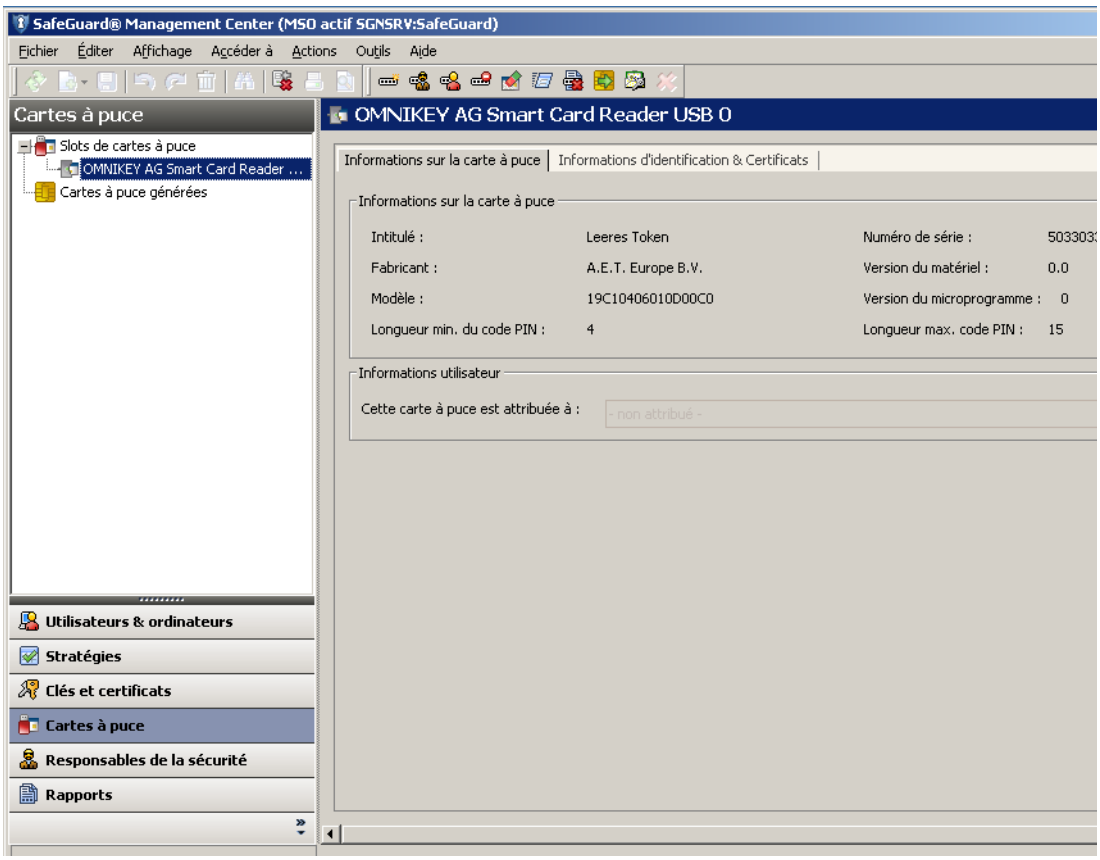
Dans la zone **Cartes à puce** de Management Center, le responsable de la sécurité peut : obtenir une présentation des clés cryptographiques et des certificats ayant été générés ; filtrer des présentations ; bloquer des cartes à puce pour l'authentification ; et lire ou supprimer les données d'une clé cryptographique.

18.11.1 Affichage des informations de la clé cryptographique/carte à puce

Si vous êtes responsable de la sécurité, vous pouvez afficher des informations concernant toutes les clés cryptographiques ou sur certaines clés cryptographiques ayant été générées, et filtrer des présentations.

Condition préalable : la clé cryptographique doit être connectée.

Dans SafeGuard Management Center, cliquez sur **Cartes à puce**.



- Informations concernant une clé cryptographique individuelle :

  Cochez la clé cryptographique concernée sous **Slots de cartes à puce**. Le fabricant, le type, le numéro de série, les données matérielles et les règles des codes PIN sont affichés sous **Informations sur la carte à puce**. Vous pouvez également voir à quel utilisateur la clé cryptographique est attribuée.

- Présentation des clés cryptographiques :

  Cochez **Cartes à puce générées**. Vous pouvez afficher toutes les cartes à puce ayant été générées ou filtrer la présentation par utilisateur. Le numéro de série de la clé cryptographique, les utilisateurs attribués et la date de génération sont affichés. Vous pouvez également voir si la clé cryptographique est bloquée.

18.11.2 Lecture des informations de la clé cryptographique/carte à puce

Si vous êtes responsable de la sécurité, vous pouvez utiliser le code PIN utilisateur généré pour la clé cryptographique pour voir les données qu'elle contient.

Condition préalable : la clé cryptographique doit être connectée. Le responsable de la sécurité doit connaître le code PIN. Ou il doit être initialisé. Pour cela, voir *Initialisation du code PIN utilisateur* en page 204.

Dans SafeGuard Management Center, cliquez sur **Cartes à puce**.

1. À gauche de la zone de navigation, sous **Slots de cartes à puce**, cochez la clé cryptographique concernée et sélectionnez l'onglet **Informations d'identification & Certificats**.
2. Cliquez sur l'icône **Obtenir les informations d'identification utilisateur** et saisissez le code PIN utilisateur de la clé cryptographique.

Les données de la clé cryptographique s'affichent.

18.11.3 Suppression des informations de la clé cryptographique/carte à puce

Si vous êtes responsable de la sécurité, vous pouvez supprimer les informations écrites sur la clé cryptographique par SafeGuard Enterprise.

Condition préalable : la clé cryptographique doit être connectée.

Dans SafeGuard Management Center, cliquez sur **Cartes à puce**.

1. Cochez la clé cryptographique concernée sous **Slots de cartes à puce**, à gauche de la zone de navigation.
2. Cliquez sur l'icône **Effacer la carte à puce** de la barre d'outils de SafeGuard Management Center.
3. Saisissez le code PIN du SO qui a été attribué à la clé cryptographique et confirmez en cliquant sur **OK**.

Toutes les données gérées par SafeGuard Enterprise sont supprimées. Les certificats restent sur la clé cryptographique.

Le code PIN de l'utilisateur est réinitialisé à 1234.

Les clés cryptographiques effacées sont ainsi automatiquement supprimées de la liste des clés cryptographiques générées.

18.11.4 Blocage d'une clé cryptographique ou carte à puce

Si vous êtes responsable de la sécurité, vous pouvez bloquer des clés cryptographiques. Ceci est pratique, par exemple, si une clé cryptographique a été perdue.

Dans SafeGuard Management Center, cliquez sur **Cartes à puce**.

1. Cochez **Cartes à puce générées** à gauche de la zone de navigation.
2. Cochez la clé cryptographique à bloquer et cliquez sur l'icône **Bloquer la carte à puce** de la barre d'outils de SafeGuard Management Center.

La clé cryptographique est bloquée pour l'authentification et l'utilisateur attribué ne peut plus l'utiliser pour se connecter. La clé cryptographique ne peut être débloquée qu'en utilisant le code PIN du SO.

19 SafeGuard Data Exchange

SafeGuard Data Exchange est utilisé pour chiffrer des données stockées sur des supports amovibles connectés à un ordinateur afin d'échanger ces données avec d'autres utilisateurs. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une interaction utilisateur minimale.

Seuls les utilisateurs disposant des clés appropriées peuvent lire le contenu des données chiffrées. Tout processus de chiffrement ultérieur est exécuté de manière transparente.

Dans le cadre d'une administration centralisée, vous définissez la gestion des données de supports amovibles.

En tant que responsable de la sécurité, vous définissez les paramètres spécifiques dans une stratégie du type **Protection du périphérique** avec *Cible de protection de périphérique* : **Supports amovibles**.

Le chiffrement basé sur fichier doit être utilisé pour SafeGuard Data Exchange.

Clés de groupe

Pour échanger des données chiffrées entre utilisateurs, des clés de groupe SafeGuard Enterprise doivent être utilisées. Si la clé de groupe se trouve dans les jeux de clés des utilisateurs, ces derniers peuvent accéder en toute transparence aux supports amovibles connectés à leurs ordinateurs.

Sur les ordinateurs sur lesquels SafeGuard Enterprise n'est pas installé, il est impossible d'accéder aux données chiffrées de supports amovibles, à l'exception de la clé de domaine/groupe définie de manière centralisée qui peut être utilisée avec la passphrase de support.

Avis : SafeGuard Portable peut être utilisé pour utiliser/partager des données chiffrées de supports amovibles sur/avec des ordinateurs/utilisateurs ne disposant pas de SafeGuard Enterprise. SafeGuard Portable nécessite l'utilisation de clés locales ou d'une passphrase de support.

Clés locales

SafeGuard Data Exchange prend en charge le chiffrement à l'aide de clés locales. Des clés locales sont créées sur les ordinateurs et peuvent être utilisées pour chiffrer des données de supports amovibles. Elles sont créées en saisissant une passphrase et sauvegardées dans la base de données de SafeGuard Enterprise.

Avis : l'utilisateur est autorisé par défaut à créer des clés locales. Si des utilisateurs ne doivent pas y être autorisés, vous devez désactiver cette option de manière explicite. Cette opération s'effectue par le biais d'une stratégie du type **Protection du périphérique** avec *Cible de protection de périphérique* : **Périphériques de stockage locaux** (**Paramètres généraux** > **L'utilisateur est autorisé à créer une clé locale :** Non).

Si des clés locales sont utilisées pour chiffrer des fichiers de supports amovibles, ces fichiers peuvent être déchiffrés à l'aide de SafeGuard Portable sur un ordinateur sur lequel SafeGuard Data Exchange n'est pas installé. À l'ouverture des fichiers avec SafeGuard Portable, l'utilisateur est invité à saisir la passphrase spécifiée lors de la création de la clé. L'utilisateur peut ouvrir le fichier s'il connaît la passphrase.

Grâce à SafeGuard Portable, chaque utilisateur connaissant la passphrase peut accéder à un fichier chiffré d'un support amovible. Il est ainsi également possible de partager des données chiffrées avec des partenaires ne disposant pas de SafeGuard Enterprise. SafeGuard Portable et la passphrase des fichiers auxquels ils doivent accéder doivent leur être fournis.

Si différentes clés locales sont utilisées pour chiffrer des fichiers de supports amovibles, vous pouvez également restreindre l'accès aux fichiers. Par exemple : Vous chiffrez les fichiers contenus sur une carte mémoire USB à l'aide d'une clé avec la passphrase *my_localkey* et chiffrez un fichier nommé *ForMyPartner.doc* à l'aide de la passphrase *partner_localkey*. Si vous donnez la carte USB à un partenaire et que vous lui fournissez la passphrase *partner_localkey*, il n'aura accès qu'au fichier *ForMyPartner.doc*.

Avis : par défaut, SafeGuard Portable est copié automatiquement sur tous les supports amovibles connectés au système. Si vous ne souhaitez pas que SafeGuard Portable soit copié automatiquement sur les supports amovibles, désactivez l'option **Copier portable SG vers support amovible** dans une stratégie du type **Chiffrement de périphérique**.

Passphrase du support

SafeGuard Data Exchange permet également de spécifier qu'une seule passphrase de support pour tous les supports amovibles (sauf les supports optiques) doit être créée sur les ordinateurs. La passphrase de support permet d'accéder à la clé de domaine/groupe définie de manière centralisée et à toutes les clés locales utilisées dans SafeGuard Portable. L'utilisateur ne saisit qu'une seule passphrase et peut accéder à tous les fichiers chiffrés dans SafeGuard Portable, quelle que soit la clé locale utilisée pour le chiffrement.

Sur chaque ordinateur, une clé de chiffrement de support unique pour le chiffrement de données est créée automatiquement pour chaque périphérique. Cette clé est protégée par la passphrase de support et une clé de domaine/groupe définie de manière centralisée. Sur un ordinateur sur lequel SafeGuard Data Exchange est installé, il n'est donc pas nécessaire de saisir la passphrase de support pour accéder aux fichiers chiffrés contenus sur le support amovible. L'accès est accordé automatiquement si la clé appropriée se trouve dans le jeu de clés de l'utilisateur.

La clé de domaine/groupe à utiliser doit être spécifiée sous **Clé définie pour le chiffrement**.

La fonction de passphrase de support est disponible lorsque l'option **L'utilisateur peut définir une passphrase de support pour les périphériques** est activée dans une stratégie du type **Protection du périphérique**.

Lorsque ce paramètre est activé sur l'ordinateur, l'utilisateur est invité automatiquement à saisir une passphrase de support lors de la première connexion au support amovible. La passphrase de support est valide sur chaque ordinateur auquel l'utilisateur peut se connecter. L'utilisateur peut également changer la passphrase de support et la synchronisation est automatique lorsque la passphrase reconnue sur l'ordinateur et la passphrase de support amovible ne correspondent pas.

En cas d'oubli de la passphrase de support, l'utilisateur peut la récupérer sans recourir au support.

Avis : pour activer la passphrase de support, activez l'option **L'utilisateur peut définir une passphrase de support pour les périphériques** dans une stratégie du type Chiffrement de périphérique.

Passphrase de support et ordinateurs finaux non gérés

Sur un ordinateur final non géré, autrement dit un ordinateur fonctionnant en mode autonome, sur lequel la fonction de passphrase de support est désactivée, aucune clé n'est disponible une fois l'installation terminée, car les ordinateurs finaux non gérés utilisent des clés locales uniquement. Avant de pouvoir utiliser le chiffrement, l'utilisateur doit créer une clé.

Si la fonction de passphrase de support est activée dans une stratégie de support amovible pour ces ordinateurs, la clé de chiffrement de support est créée automatiquement sur l'ordinateur et peut être utilisée pour un chiffrement immédiatement après l'installation. Il s'agit d'une clé prédéfinie du jeu de clés de l'utilisateur et s'affiche sous la forme d'un `<nom d'utilisateur>` dans les boîtes de dialogue de sélection de clé.

Le cas échéant, les clés de chiffrement de support sont également utilisées pour toutes les tâches de chiffrement initial.

19.1 Pratique recommandée

Cette section décrit des études de cas classiques de SafeGuard Enterprise et comment les mettre en œuvre en créant les stratégies appropriées.

Bob et Alice sont deux employés de la même société et disposent de SafeGuard Data Exchange. Joe est un partenaire externe et ne dispose pas de SafeGuard Enterprise sur son PC.

19.1.1 Utilisation interne uniquement

Bob souhaite partager des données chiffrées sur un support amovible avec Alice. Ils font partie du même groupe et disposent donc de la clé de groupe appropriée dans leur jeu de clés SafeGuard Enterprise. Étant donné qu'ils utilisent la même clé de groupe, ils peuvent accéder en toute transparence aux fichiers chiffrés sans saisir de passphrase.

Vous devez définir les paramètres dans une stratégie du type **Protection du périphérique\Supports amovibles** :

- **Mode de chiffrement du support** : basé sur fichier
- **Clé à utiliser pour le chiffrement** : Clé définie dans la liste
  - Clé définie dans la liste : <clé de groupe/domaine > (par ex. group_users_Bob_Alice@DC=...)
    pour s'assurer qu'ils partagent la même clé

Si les stratégies de l'entreprise définissent également que tous les fichiers des supports amovibles doivent toujours être chiffrés, ajoutez les paramètres suivants :

- **Chiffrement initial de tous les fichiers** : Oui
  Vérifie que les fichiers des supports amovibles sont chiffrés lors de la première connexion du support au système.
- **L'utilisateur peut annuler le chiffrement initial** : Non
  L'utilisateur ne peut pas annuler le chiffrement initial, pour le différer par exemple.
- **L'utilisateur est autorisé à accéder aux fichiers non chiffrés** : Non
  Si des fichiers au format brut sont détectés sur le support amovible, leur accès est refusé.
- **L'utilisateur peut déchiffrer des fichiers** : Non
  L'utilisateur n'est pas autorisé à déchiffrer des fichiers de supports amovibles.
- **Copier portable SG vers support amovible** : Non
  SafeGuard Portable n'est pas nécessaire tant que les données de supports amovibles sont partagées dans un groupe de travail. SafeGuard Portable permet également d'autoriser le déchiffrement de fichiers sur des ordinateurs sur lesquels SafeGuard Enterprise n'est pas installé.

Les utilisateurs peuvent partager des données en échangeant simplement leurs périphériques. Lorsqu'ils connectent les périphériques à leurs ordinateurs, ils accèdent en toute transparence aux fichiers chiffrés.

Avis : ce cas d'utilisation est possible grâce à SafeGuard Enterprise Device Encryption avec lequel l'ensemble du périphérique amovible est chiffré par secteur.

19.1.2 Utilisation à domicile ou personnelle sur un PC tiers

À domicile :

Bob souhaite utiliser son support amovible chiffré sur son PC personnel, sur lequel SafeGuard Enterprise n'est pas installé. Sur son PC personnel, Bob déchiffre les fichiers avec SafeGuard Portable. En définissant une passphrase de support pour tous les supports amovibles de Bob, il ouvre simplement SafeGuard Portable et saisit la passphrase de support. Il a ensuite accès de manière transparente à tous les fichiers chiffrés, quelle que soit la clé utilisée pour les chiffrer.

Utilisation personnelle sur un PC tiers :

Bob connecte le périphérique amovible à l'ordinateur de Joe (partenaire externe) et saisit la passphrase de support pour accéder aux fichiers chiffrés stockés sur le périphérique. Bob peut alors copier les fichiers (chiffrés ou non) sur l'ordinateur de Joe.

Comportement sur l'ordinateur final

- Bob connecte pour la première fois le périphérique amovible.
- La clé de chiffrement de support, unique pour chaque périphérique, est créée automatiquement.
- Bob est invité à saisir la passphrase de support pour l'utiliser hors ligne via SG Portable.
- L'utilisateur n'a pas besoin de connaître les clés utilisées ou le jeu de clés. La clé de chiffrement de support est toujours utilisée pour le chiffrement de données sans aucune interaction de l'utilisateur. La clé de chiffrement de support n'est pas visible, y compris pour l'utilisateur. Seule la clé de groupe/domaine définie de manière centralisée est visible.
- Bob et Alice, du même groupe ou domaine, accèdent de manière transparente car ils partagent la même clé de groupe/domaine.
- Si Bob souhaite accéder à des fichiers chiffrés d'un périphérique amovible sur un ordinateur sur lequel SafeGuard Data Exchange n'est pas installé, il peut utiliser la passphrase de support dans SafeGuard Portable.

Vous devez définir les paramètres dans une stratégie du type **Protection du périphérique\Supports amovibles** :

- **Mode de chiffrement du support** : basé sur fichier
- **Clé à utiliser pour le chiffrement** : Clé définie dans la liste
  - Clé définie dans la liste : <clé de groupe/domaine > (par ex. group_users_Bob_Alice@DC=...)
    pour s'assurer qu'ils partagent la même clé.
- **L'utilisateur peut définir une passphrase de support pour les périphériques** : Oui
  L'utilisateur définit une passphrase de support sur son ordinateur qui s'applique à tous ses supports amovibles.
- **Copier portable SG vers support amovible** : Oui
  SafeGuard Portable permet à l'utilisateur d'accéder à tous les fichiers chiffrés du support amovible en saisissant une passphrase de support unique sur un système sur lequel SafeGuard Data Exchange n'est pas installé.

Si les stratégies de l'entreprise définissent également que tous les fichiers des supports amovibles doivent toujours être chiffrés, ajoutez les paramètres suivants :

- **Chiffrement initial de tous les fichiers** : Oui
  Vérifie que les fichiers des supports amovibles sont chiffrés lors de la première connexion du support au système.
- **L'utilisateur peut annuler le chiffrement initial** : Non
  L'utilisateur ne peut pas annuler le chiffrement initial, pour le différer par exemple.
- **L'utilisateur est autorisé à accéder aux fichiers non chiffrés** : Non
  Si des fichiers au format brut sont détectés sur le support amovible, leur accès est refusé.
- **L'utilisateur peut déchiffrer des fichiers** : Non
  L'utilisateur n'est pas autorisé à déchiffrer des fichiers de supports amovibles.

Au bureau, Bob et Alice accèdent de manière transparente aux fichiers chiffrés du support amovible. Sur leur PC personnel ou sur un PC tiers, ils peuvent utiliser SafeGuard Portable pour ouvrir des fichiers chiffrés. Les utilisateurs saisissent simplement la passphrase de support et peuvent accéder à tous les fichiers chiffrés. Cette méthode simple mais fiable permet de chiffrer des données sur chaque support amovible. Cette configuration vise à réduire au maximum l'interaction de l'utilisateur tout en chiffrant chaque fichier d'un support amovible et en permettant aux utilisateurs d'accéder hors ligne aux fichiers chiffrés. L'utilisateur n'est pas autorisé à déchiffrer des fichiers de supports amovibles.

Avis : dans cette configuration, les utilisateurs ne sont pas autorisés à créer des clés locales car elles sont inutiles dans ce cas de figure. Ceci doit être spécifié dans une stratégie du type **Protection du périphérique** avec Cible de protection de périphérique : **Périphériques de stockage locaux** (**Paramètres généraux > L'utilisateur est autorisé à créer une clé locale** : Non).

- **Copier portable SG vers support amovible** : Non
  SafeGuard Portable n'est pas nécessaire tant que les données de supports amovibles sont partagées dans un groupe de travail. SafeGuard Portable permet également d'autoriser le déchiffrement de fichiers sur des ordinateurs sur lesquels SafeGuard Enterprise n'est pas installé.

Au bureau, l'utilisateur accède de manière transparente aux fichiers chiffrés d'un support amovible. À son domicile, il utilise SafeGuard Portable pour ouvrir des fichiers chiffrés. L'utilisateur saisit simplement la passphrase de support et accède à tous les fichiers chiffrés, quelle que soit la clé de chiffrement utilisée.

19.1.3 Partage d'un support amovible avec un tiers externe

Bob souhaite partager un périphérique chiffré avec Joe (tiers externe) qui ne dispose pas de SG Data Exchange et qui doit donc utiliser SG Portable. Si Bob ne souhaite pas que Joe accède à tous les fichiers chiffrés du support amovible, il peut créer une clé locale et chiffrer les fichiers avec cette clé. Joe peut alors utiliser SG Portable et ouvrir les fichiers chiffrés à l'aide de la passphrase de la clé locale et Bob peut toujours utiliser la passphrase de support pour accéder aux fichiers chiffrés du support amovible.

Comportement sur l'ordinateur final

- Bob connecte pour la première fois le périphérique amovible.
  La clé de chiffrement de support, propre à chaque périphérique, est créée automatiquement.
- Bob est invité à saisir la passphrase de support pour l'utiliser hors ligne.
- La clé de chiffrement de support est utilisée pour le chiffrement de données sans aucune interaction de l'utilisateur, mais...
- Bob peut maintenant créer ou sélectionner une clé locale (appelée JoeKey par exemple) pour chiffrer des fichiers spécifiques à échanger avec Joe.
- Bob et Alice, du même groupe ou domaine, accèdent de manière transparente car ils partagent la même clé de groupe/domaine.
- Si Bob souhaite accéder à des fichiers chiffrés d'un périphérique amovible sur un ordinateur sur lequel SafeGuard Data Exchange n'est pas installé, il peut utiliser la passphrase de support dans SafeGuard Portable.
- Joe peut accéder aux fichiers spécifiques en saisissant la passphrase de la clé (JoeKey) sans accéder à l'ensemble des fichiers du support amovible.

Vous devez définir les paramètres dans une stratégie du type **Protection du périphérique\Supports amovibles** :

- **Mode de chiffrement du support :** basé sur fichier
- **Clé à utiliser pour le chiffrement** : Toute clé du jeu de clés utilisateur
  Permet à l'utilisateur de choisir différentes clés pour chiffrer des fichiers de son support amovible.
  - **Clé définie pour le chiffrement** : <clé de groupe/domaine > (par ex. group_users_Bob_Alice@DC=...)
    L'utilisateur peut partager des données dans son groupe de travail et permettre à un autre utilisateur d'accéder de manière transparente au support amovible lorsqu'il le connecte à son ordinateur professionnel.
- **L'utilisateur peut définir une passphrase de support pour les périphériques**: Oui
  L'utilisateur définit une passphrase de support sur son ordinateur qui s'applique à tous ses supports amovibles.
- **Copier portable SG vers support amovible** : Oui
  SafeGuard Portable permet à l'utilisateur d'accéder à tous les fichiers chiffrés du support amovible en saisissant une passphrase de support unique sur un système sur lequel SafeGuard Data Exchange n'est pas installé.

Si les stratégies de l'entreprise définissent également que tous les fichiers des supports amovibles doivent toujours être chiffrés, ajoutez les paramètres suivants :

- **Chiffrement initial de tous les fichiers** : Oui
  Vérifie que les fichiers des supports amovibles sont chiffrés lors de la première connexion du support au système.
- **L'utilisateur peut annuler le chiffrement initial** : Non
  L'utilisateur ne peut pas annuler le chiffrement initial, pour le différer par exemple.
- **L'utilisateur est autorisé à accéder aux fichiers non chiffrés** : Non
  Si des fichiers au format brut sont détectés sur le support amovible, leur accès est refusé.
- **L'utilisateur peut déchiffrer des fichiers** : Non
  L'utilisateur n'est pas autorisé à déchiffrer des fichiers de supports amovibles.

Au bureau, Bob et Alice accèdent de manière transparente aux fichiers chiffrés du support amovible. À leur domicile, ils peuvent utiliser SafeGuard Portable pour ouvrir des fichiers chiffrés en saisissant la passphrase de support. Si Bob ou Alice souhaite partager le support amovible sur un PC tiers sur lequel SafeGuard Data Exchange n'est pas installé, ils peuvent utiliser des clés locales pour s'assurer que le tiers externe n'accède qu'à certains fichiers. Cette configuration avancée implique une interaction plus importante de l'utilisateur en l'autorisant à créer des clés locales sur son ordinateur.

Avis : pour ce faire, l'utilisateur doit au préalable être autorisé à créer des clés locales (paramètre par défaut dans SafeGuard Enterprise).

20 Authentification au démarrage (POA)

SafeGuard Enterprise identifie l'utilisateur avant même le démarrage du système d'exploitation. Pour cela, le noyau du système de SafeGuard Enterprise démarre en amont. Il est protégé contre toute modification puis il est enregistré et masqué sur le disque dur. Ce n'est que lorsque l'utilisateur s'est correctement authentifié à partir de l'authentification au démarrage que le système d'exploitation (Windows) réel démarre à partir de la partition chiffrée. L'utilisateur est ensuite automatiquement connecté à Windows. La procédure est identique lorsque l'ordinateur final revient du mode hibernation.

Les avantages de l'authentification au démarrage de SafeGuard Enterprise sont les suivants :

- une interface utilisateur graphique, avec prise en charge de la souris et des fenêtres pouvant être déplacées, pour plus de facilité et de lisibilité ;
- une présentation graphique qui, en suivant les instructions, peut être personnalisée pour les ordinateurs d'entreprise (image d'arrière-plan, image de connexion, message d'accueil, etc.) ;
- la prise en charge de nombreux lecteurs de cartes et d'un grand nombre de cartes à puce ;
- la prise en charge des comptes utilisateur Windows et des mots de passe dès l'étape de préinitialisation, ce qui évite à l'utilisateur de devoir mémoriser des informations d'identification distinctes ;
- la prise en charge de format Unicode et par conséquent des mots de passe et des interfaces utilisateur en langue étrangère.

20.1 Connexion

SafeGuard Enterprise fonctionne avec une connexion basée sur certificat. Les utilisateurs ont besoin de clés et de certificats pour se connecter lors de l'authentification au démarrage. Toutefois, la clé et les certificats spécifiques d'un utilisateur ne sont générés que lorsque celui-ci est parvenu à se connecter à Windows. En d'autres termes, seuls les utilisateurs qui se sont connectés à Windows peuvent également s'authentifier lors de l'authentification au démarrage.

Pour clarifier la manière dont un utilisateur se connecte à SafeGuard Enterprise, vous trouverez ci-après une brève introduction. Pour obtenir une description détaillée des procédures de connexion d'authentification au démarrage, consultez l'aide de l'utilisateur de SafeGuard Enterprise.

Remarque: Sous Windows Vista, les utilisateurs doivent tout d'abord appuyer sur les touches **CTRL+ALT+SUPPR** pour démarrer la connexion automatique et la connexion. L'administrateur peut désactiver ce paramètre dans la console MMC de l'éditeur d'objet de stratégie de groupe sous **Paramètres Windows > Paramètres de sécurité > Stratégies locales > Désactiver les options de sécurité** (Enregistrement interactif : **CTRL+ ALT+SUPPR** non nécessaire).

20.1.1 Connexion SafeGuard automatique

Lors de la première connexion, la fenêtre de connexion automatique à SafeGuard Enterprise s'affiche après le démarrage de l'ordinateur final.

Que se passe-t-il ?

1. Un utilisateur automatique est connecté.
2. Le client est enregistré automatiquement sur le serveur SGN.
3. La clé machine est envoyée au serveur SGN et stockée dans la base de données SGN.
4. Les stratégies de la machine sont envoyées à l'ordinateur final.

20.1.2 Connexion Windows

La boîte de dialogue de connexion Windows apparaît. L'utilisateur se connecte.

Que se passe-t-il ?

1. L'ID de l'utilisateur et le mot de passe chiffré sont envoyés au serveur.
2. Les stratégies, certificats et clés utilisateur sont créés et envoyés à l'ordinateur final.
3. POA est activé.

20.1.3 Connexion d'authentification au démarrage

Lorsque l'ordinateur final redémarre, l'authentification au démarrage apparaît.

Que se passe-t-il ?

1. Les certificats et les clés sont disponibles pour l'utilisateur, et il peut se connecter lors de l'authentification au démarrage.
2. Toutes les données sont chiffrées et sécurisées avec la clé publique RSA de l'utilisateur.
3. Tous les autres utilisateurs qui souhaitent se connecter doivent, au préalable, être importés dans POA.

20.1.4 Retard de connexion

Sur un ordinateur protégé par SafeGuard Enterprise, un retard de connexion s'applique si un utilisateur fournit des informations d'identification incorrectes pendant l'authentification Windows ou l'authentification au démarrage. Le retard de connexion augmente à chaque échec de tentative de connexion. Après un échec de connexion, une boîte de dialogue apparaît et affiche le délai restant.

Remarque: Si un utilisateur saisit un code PIN incorrect lors de la connexion sur la carte à puce, il n'y aura aucun retard de connexion.

Vous pouvez indiquer le nombre de tentatives de connexion autorisées dans une stratégie du type **Authentification** en vous aidant pour cela de l'option **Nbre maximum d'échecs de connexion**.

20.1.5 Verrouillage de la machine

Dans une stratégie du type **Authentification**, vous pouvez également spécifier le verrouillage de l'ordinateur après un certain nombre d'échecs de tentatives de connexion en définissant l'option **Verrouiller la machine** sur **Oui**. Pour déverrouiller leur ordinateur, les utilisateurs doivent lancer une procédure Challenge/Réponse.

20.2 Importation d'autres utilisateurs

Le premier utilisateur à se connecter à Windows est enregistré automatiquement dans l'authentification au démarrage. Aucun autre utilisateur Windows ne peut alors se connecter à l'authentification au démarrage.

Les autres utilisateurs doivent être importés avec l'aide du premier. Pour obtenir une description détaillée de l'importation d'autres utilisateurs, consultez l'aide de l'utilisateur de SafeGuard Enterprise.

Un paramètre de stratégie spécifie qui est autorisé à importer un nouvel utilisateur. Vous pouvez trouver cette stratégie dans Management Center sous

Éléments de stratégie

- Type : Spécifique à l'ordinateur
- Champ : Importation de nouveaux utilisateurs autorisée pour

Paramètre par défaut : propriétaire

Le propriétaire d'un ordinateur final est spécifié dans Management Center sous

Utilisateurs & ordinateurs

- Cochez <nom de l'ordinateur final>
- Onglet Utilisateurs

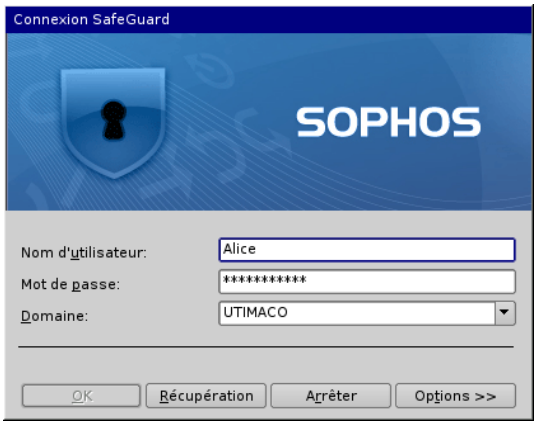
Remarque: Pour des ordinateurs finaux non gérés, c'est-à-dire des ordinateurs finaux fonctionnant en mode autonome, SafeGuard Enterprise propose des comptes d'accès POA. Les comptes d'accès POA sont des comptes locaux prédéfinis qui permettent aux utilisateurs de se connecter (connexion POA) à des ordinateurs finaux, une fois l'authentification au démarrage activée, pour effectuer des tâches administratives Les comptes sont définis dans la zone **Utilisateur & ordinateurs** de SafeGuard Management Center (nom d'utilisateur et mot de passe) et affectés aux ordinateurs finaux via des groupes d'accès POA inclus dans les packages de configuration.

Remarque: Pour des informations détaillées sur les comptes de service, reportez-vous à voir *Comptes d'accès POA pour la connexion POA sur des ordinateurs finaux non gérés*, à la page 4.

20.3 Configuration de l'authentification au démarrage

La boîte de dialogue POA comporte les composants suivants :

- Image de connexion
- Texte des boîtes de dialogue
- Langue de la disposition du clavier



Vous pouvez modifier l'apparence de la boîte de dialogue de l'authentification au démarrage selon vos préférences, grâce notamment aux paramètres de stratégie de SafeGuard Management Center.

20.3.1 Image d'arrière-plan et de connexion

Par défaut, les images d'arrière-plan et de connexion qui s'affichent dans l'authentification au démarrage sont conçues selon SafeGuard. Toutefois, il est possible d'afficher des images différentes telles que le logo de l'entreprise.

Les images d'arrière-plan et de connexion sont définies via une stratégie du type **Paramètres généraux**.

Utilisées dans SafeGuard Enterprise, les images d'arrière-plan et de connexion doivent respecter certaines conditions :

Image d'arrière-plan

Taille de fichier maximale pour toutes les images d'arrière-plan : **500 Ko**

SafeGuard Enterprise prend en charge deux variantes d'images d'arrière-plan :

- **1024 x 768** (mode VESA)

  Couleurs : aucune restriction

  Option dans le type de stratégie **Paramètres généraux : Image d'arrière-plan dans POA**

- **640 x 480** (mode VGA)

  Couleurs : 16

  Option dans le type de stratégie **Paramètres généraux : Image d'arrière-plan dans POA (basse résolution)**

Image de connexion

Taille de fichier maximale pour toutes les images de connexion : **100 Ko**

SafeGuard Enterprise prend en charge deux variantes d'images de connexion :

- **413 x 140**

  Couleurs : aucune restriction

  Option dans le type de stratégie **Paramètres généraux : Image de connexion dans POA**

- **413 x 140**

  Couleurs : 16

  Option dans le type de stratégie **Paramètres généraux : Image de connexion dans POA (basse résolution)**

Les images, les textes d'informations et les listes doivent être créés en premier sous la forme de fichiers (fichiers BMP, PNG, JPG ou texte), puis enregistrés dans la fenêtre de navigation.

20.3.1.1 Enregistrement d'images

Pour enregistrer des images, procédez comme suit :

1. Dans la zone de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Images** et sélectionnez **Nouveau** > **Image**.
2. Entrez le nom de l'image dans le champ **Nom de l'image**.

3. Cliquez sur **[...]** pour sélectionner l'image préalablement créée.
4. Cliquez sur **OK**.

La nouvelle image apparaît en tant que nœud secondaire de **Images** dans la zone de navigation de stratégie. Si vous sélectionnez l'image, elle s'affiche dans la zone d'action. L'image peut désormais être sélectionnée lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres images. Toutes les images enregistrées s'affichent en tant que nœuds secondaires.

Remarque: Grâce au bouton **Modifier l'image**, vous pouvez changer l'image attribuée. Une boîte de dialogue de sélection d'une autre image s'affiche lorsque vous cliquez sur ce bouton.

20.3.2 Texte des informations défini par l'utilisateur dans l'authentification au démarrage (POA)

Vous pouvez personnaliser l'authentification au démarrage (POA) en affichant les **textes d'informations définis par l'utilisateur** :

- Texte d'informations affiché lors du lancement d'une procédure de Challenge/Réponse pour la récupération de connexion (p. ex. : « Contactez le bureau de support en appelant au 01234-56789. »)

  Option dans le type de stratégie **Paramètres généraux : Texte d'informations**

- Mentions légales affichées après la connexion à POA

  Option dans le type de stratégie **Paramètres de machine spécifiques : Texte de la mention légale**

- Texte d'informations supplémentaires affiché après la connexion à POA

  Option dans le type de stratégie **Paramètres de machine spécifiques : Texte des informations supplémentaires**

20.3.2.1 Enregistrement de textes d'informations

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans SafeGuard Management Center. La taille maximale de ces fichiers pour les textes d'informations est de **50 Ko**. SafeGuard Enterprise n'utilise que des textes codés en Unicode UTF-16. Si vous ne créez pas les fichiers texte dans ce format, ils sont convertis automatiquement lors de l'enregistrement.

Si une conversion s'impose, un message s'affiche et indique que le fichier est en cours de conversion.

Pour enregistrer des textes d'informations :

1. Dans la zone de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Texte d'informations** et sélectionnez **Nouveau > Texte**.
2. Entrez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.
3. Cliquez sur **[...]** pour sélectionner le fichier texte préalablement créé. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Texte d'informations** dans la zone de navigation de stratégie. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

Remarque: Grâce au bouton **Modifier le texte**, vous pouvez ajouter du texte au texte existant. Une boîte de dialogue de sélection d'un autre fichier texte s'affiche lorsque vous cliquez sur ce bouton. Le texte contenu dans ce fichier est ajouté à la fin du texte existant.

20.3.3 Langue du texte de la boîte de dialogue d'authentification au démarrage

Après l'installation du logiciel de chiffrement SafeGuard Enterprise, le texte de la boîte de dialogue d'authentification au démarrage est affiché dans la langue par défaut, celle qui a été définie dans les Options régionales et linguistiques de Windows sur l'ordinateur final, lors de l'installation de SafeGuard Enterprise.

Après l'installation, la langue dans laquelle le texte de la boîte de dialogue d'authentification au démarrage s'affiche ne peut être modifiée que via une stratégie définie dans SafeGuard Management Center. Le changement de la langue par défaut sous Windows n'affecte pas celle du texte de la boîte de dialogue d'authentification au démarrage.

La langue du texte de la boîte de dialogue d'authentification au démarrage est définie via une stratégie du type **Paramètres généraux** (option **Langue utilisée sur le client**).

20.3.4 Disposition du clavier

Chaque pays ou presque a une disposition de clavier qui lui est propre, c'est-à-dire une répartition différente des touches. La disposition du clavier dans POA est importante lorsque vous saisissez des noms d'utilisateur, des mots de passe et des codes de réponse.

Par défaut, pour l'authentification au démarrage, SafeGuard Enterprise adopte la disposition du clavier qui a été définie dans les Options régionales et linguistiques de Windows pour l'utilisateur Windows par défaut, au moment de l'installation de SafeGuard Enterprise. Si « Allemand » est la disposition de clavier définie sous Windows, la disposition allemande du clavier sera utilisée dans POA.

La langue de la disposition du clavier utilisée est affichée dans POA, par exemple « FR » pour le français. Outre la disposition du clavier par défaut, la disposition du clavier américain (anglais) peut également être utilisée.

Il existe un certain nombre d'exceptions :

- La disposition du clavier est effectivement prise en charge, mais la police requise est manquante (Bulgare, par exemple). Par conséquent, seuls les caractères spéciaux sont affichés dans le champ **Nom d'utilisateur**.
- Aucune disposition du clavier n'est disponible (par exemple pour la République Dominicaine). Dans ces situations, POA revient à la disposition de clavier d'origine. Pour la République Dominicaine, il s'agit de l'« espagnol ».

Remarque: Toutes les dispositions de clavier non prises en charge utilisent la disposition de clavier américain par défaut. Cela signifie également que les seuls caractères reconnus et pouvant être saisis au clavier sont ceux qui sont pris en charge dans la disposition de clavier américain. De la sorte, les utilisateurs ne peuvent se connecter lors de l'authentification au démarrage que si leur nom d'utilisateur et leur mot de passe sont composés de caractères pris en charge dans la disposition de clavier de la langue correspondante.

20.3.4.1 Clavier virtuel

SafeGuard Enterprise propose aux utilisateurs un clavier virtuel qu'ils peuvent afficher/masquer dans l'authentification au démarrage et sur les touches à l'écran duquel ils peuvent cliquer pour entrer des informations d'identification, etc.

En tant que responsable de la sécurité, vous pouvez activer/désactiver l'affichage du clavier virtuel à l'aide d'une stratégie du type **Paramètres de machine spécifiques** avec l'option **Clavier virtuel**.

La prise en charge du clavier virtuel doit être activée/désactivée via un paramètre de stratégie.

Le clavier virtuel accepte différentes dispositions et il est possible de changer la disposition à l'aide des mêmes options que pour la disposition du clavier de l'authentification au démarrage.

20.3.4.2 Modification de la disposition du clavier

La disposition du clavier pour l'authentification au démarrage, clavier virtuel inclus, peut être modifiée rétrospectivement.

Pour modifier la langue de la disposition du clavier, procédez comme suit :

1. Sélectionnez **Démarrer > Panneau de configuration > Options régionales et linguistiques > Options avancées**.
2. Dans l'onglet **Options régionales**, sélectionnez la langue souhaitée.
3. Dans l'onglet **Options avancées**, activez l'option **Appliquer tous les paramètres au compte d'utilisateur actuel et au profil utilisateur par défaut** sous **Paramètres par défaut du compte d'utilisateur**.
4. Cliquez sur **OK** pour confirmer vos paramètres.

POA mémorise la disposition du clavier utilisée au cours de la dernière connexion et l'active automatiquement à la connexion suivante. Cette opération nécessite que vous redémarriez l'ordinateur final deux fois. Si la disposition du clavier mémorisée est désactivée via les **Options régionales et linguistiques**, elle est conservée jusqu'à ce que l'utilisateur en sélectionne une autre.

Remarque: Par ailleurs, vous devez modifier la langue de la disposition du clavier pour les programmes non-unicode.

Si la langue souhaitée n'est pas disponible sur le système, Windows peut vous inviter à l'installer. Après l'avoir fait, vous devez réinitialiser l'ordinateur deux fois de sorte que, en premier lieu, la nouvelle disposition du clavier puisse être lue par l'authentification au démarrage et, en second lieu, que l'authentification au démarrage puisse définir la nouvelle disposition.

Vous pouvez changer la disposition du clavier requise pour l'authentification au démarrage à l'aide de la souris ou du clavier (**Alt+Maj**).

Vous pouvez voir les langues installées et disponibles sur le système via Démarrer > Exécuter > regedit > HKEY_USERS\.DEFAULT\Keyboard Layout\Preload.

20.4 Raccourcis clavier pris en charge dans l'authentification au démarrage

Certains paramètres et fonctionnalités matériels peuvent générer des problèmes lors du démarrage des ordinateurs finaux et provoquer le blocage du système. L'authentification au démarrage prend en charge plusieurs raccourcis clavier pour modifier les paramètres matériels et désactiver des fonctionnalités. De plus, des listes « grise » et « noire » contenant les fonctions connues pour provoquer des problèmes sont intégrées au fichier .msi installé sur l'ordinateur.

Nous vous recommandons d'installer une version mise à jour du fichier de configuration POA avant tout déploiement important de SafeGuard Enterprise. Le fichier est mis à jour tous les mois et est téléchargeable à l'adresse suivante : ftp://POACFG:POACFG@ftp.ou.utimaco.de

Vous pouvez personnaliser ce fichier en fonction du matériel d'un environnement spécifique.

Remarque: Lorsqu'un fichier personnalisé est utilisé, celui-ci remplace le fichier intégré au fichier .msi. Le fichier par défaut est utilisé uniquement lorsqu'aucun fichier de configuration POA n'a été défini ou trouvé.

Pour installer le fichier de configuration POA, entrez la commande suivante :

MSIEXEC /i <package MSI client> POACFG=<chemin du fichier de configuration POA>

Pour en savoir plus, consultez la base de connaissances : http://www.sophos.com/support/knowledgebase/article/65700.html.

Les raccourcis clavier suivants sont pris en charge dans POA :

- **Maj F3** = support patrimonial USB (actif/inactif)
- **Maj F4** = mode graphique VESA (actif/inactif)
- **Maj F5** = support USB 1.x et 2.0 (actif/inactif)
- **Maj F6** = contrôleur ATA (actif/inactif)
- **Maj F7** = support USB 2.0 seulement (actif/inactif)

  Le support USB 1.x reste tel qu'il est défini par Maj F5.
- **Maj F9** = ACPI/APIC (actif/inactif)

Matrice de dépendance des raccourcis clavier USB

Maj F3	Maj F5	Maj F7	Patrimonial	USB 1.x	USB 2.0	Commentaire
désactivé	désactivé	désactivé	activé	activé	activé	3.
activé	désactivé	désactivé	désactivé	activé	activé	Par défaut
désactivé	activé	désactivé	activé	désactivé	désactivé	1., 2.
activé	activé	désactivé	activé	désactivé	désactivé	1., 2.
désactivé	désactivé	activé	activé	activé	désactivé	3.
activé	désactivé	activé	désactivé	activé	désactivé	
désactivé	activé	activé	activé	désactivé	désactivé	
activé	activé	activé	activé	désactivé	désactivé	2.

1. Maj F5 désactive USB 1.x et USB 2.0.

Remarque: Le fait d'appuyer sur Maj F5 pendant la période d'initialisation réduit considérablement la durée de lancement de l'authentification au démarrage. Gardez cependant en mémoire que si l'ordinateur est équipé d'un clavier USB ou d'une souris USB, ces derniers peuvent être désactivés si vous appuyez sur **Maj F5**.

2. Si aucun support USB n'est actif, l'authentification au démarrage tente d'utiliser BIOS SMM au lieu de sauvegarder et de restaurer le contrôleur USB. Le legacy mode peut fonctionner dans ce scénario.

3. Le support patrimonial est actif, USB est actif. L'authentification au démarrage tente de sauvegarder et de restaurer le contrôleur USB. Il se peut que le système se bloque selon la version du BIOS utilisée.

Vous pouvez spécifier les modifications pouvant être effectuées en utilisant des raccourcis clavier lors de l'installation du logiciel de chiffrement SafeGuard Enterprise à l'aide d'un fichier .mst. Pour ce faire, utilisez l'appel approprié avec msiexec.

NOVESA	Définit si le mode VESA ou VGA est utilisé.0 = mode VESA (standard)1 = mode VGA
NOLEGACY	Définit si le support patrimonial est activé après connexion à l'authentification au démarrage.0 = support patrimonial activé 1 = le support patrimonial non activé (standard)
ALTERNATE	Définit si les périphériques USB sont pris en charge par POA. 0 = support USB activé (standard)1 = aucun support USB
NOATA	Définit si un pilote de périphérique int13 est utilisé.0 = pilote de périphérique ATA standard (par défaut)1 = pilote de périphérique int13

ACPIAPIC	Définit si le support ACPI/APIC est utilisé.0 = aucun support ACPI/APIC (par défaut)1 = support ACPI/APIC actif
NOVESA	Définit si le mode VESA ou VGA est utilisé.0 = mode VESA (standard)1 = mode VGA

20.5 POA désactivé et Lenovo Rescue and Recovery

Si l'authentification au démarrage est désactivée sur l'ordinateur, l'authentification Rescue and Recovery doit être activée pour la protection contre l'accès aux fichiers chiffrés à partir de l'environnement Rescue and Recovery.

Pour plus de détails sur l'activation de l'authentification Rescue and Recovery, veuillez vous reporter à la documentation Lenovo Rescue and Recovery.

21 Options de récupération

SafeGuard Enterprise propose plusieurs options de récupération, adaptées à différents scénarios :

- **Récupération de connexion via Local Self Help**

  Local Self Help permet aux utilisateurs ayant oublié leur mot de passe de se connecter à leur ordinateur sans l'aide du support. Les utilisateurs peuvent accéder de nouveau à leur ordinateur même si aucune connexion téléphonique ou réseau n'est disponible (à bord d'un avion, par exemple). Pour se connecter, ils doivent répondre à un certain nombre de questions prédéfinies dans l'authentification au démarrage.

  Local Self Help réduit le nombre d'appels de récupération de connexion, et ainsi les tâches de routine des membres du support en leur permettant de se concentrer sur des demandes plus complexes.

  Pour en savoir plus voir *Récupération via Local Self Help* , page 232.

- **Récupération par Challenge/Réponse**

  Le mécanisme Challenge/Réponse est un système de récupération de connexion sécurisé et fiable qui vient en aide aux utilisateurs qui ne peuvent pas se connecter à leur ordinateur ou accéder aux données chiffrées. Lors de la procédure Challenge/Réponse, l'utilisateur communique le code de challenge généré sur l'ordinateur final au responsable du support qui générera à son tour un code de réponse. Ce code autorisera l'utilisateur à exécuter une action spécifique sur l'ordinateur.

  Grâce à la récupération par Challenge/Réponse, SafeGuard Enterprise propose plusieurs flux de travail pour les scénarios de récupération classiques nécessitant l'aide du support.

  Pour en savoir plus, voir *Récupération via Challenge/Réponse* , page 238.

- **Récupération du système**

  SafeGuard Enterprise propose plusieurs méthodes et outils de récupération relatifs à des composants du système essentiels ainsi qu'à des composants SafeGuard Enterprise, par exemple :

  - MBR (Master Boot Record) corrompu
  - Problèmes du noyau SafeGuard Enterprise
  - Problèmes d'accès aux volumes
  - Problèmes d'initialisation Windows
  - Problèmes GINA

Pour en savoir plus, voir *Récupération du système* , page 263.

22 Récupération via Local Self Help

SafeGuard Enterprise propose Local Self Help pour les ordinateurs protégés par SafeGuard Enterprise afin de permettre aux utilisateurs ayant oublié leur mot de passe de se connecter à leur ordinateur sans recourir à l'aide du support.

Grâce à Local Self Help, les utilisateurs peuvent accéder de nouveau à leur ordinateur portable dans les situations où aucune connexion par téléphone ou réseau n'est disponible et où ils ne peuvent donc pas utiliser de procédure Challenge/Réponse (par exemple à bord d'un avion). L'utilisateur peut se connecter à son ordinateur en répondant à un nombre prédéfini de questions dans l'authentification au démarrage (POA).

En tant que responsable de la sécurité, vous pouvez définir de manière centralisée les questions auxquelles il faudra répondre et les distribuer sur l'ordinateur à l'aide d'une stratégie. À titre d'exemple, nous vous proposons un sujet de question prédéfini. Vous pouvez utiliser ce sujet tel quel ou le modifier. Dans la stratégie correspondante, vous pouvez également accorder aux utilisateurs le droit de définir des questions personnalisées.

Pour proposer les réponses initiales et modifier les questions, l'assistant de Local Self Help est disponible sur l'ordinateur final une fois que la fonction est activée à l'aide d'une stratégie. Pour obtenir une description détaillée de Local Self Help sur l'ordinateur final, consultez l'aide de l'utilisateur de SafeGuard Enterprise, chapitre *Récupération via Local Self Help*.

Local Self Help réduit le nombre d'appels de récupération de connexion, et ainsi les tâches de routine des membres du support en leur permettant de se concentrer sur des demandes plus complexes.

22.1 Définition des paramètres de Local Self Help à l'aide d'une stratégie

Vous définissez les paramètres de Local Self Help dans une stratégie du type **Paramètres généraux** sous **Récupération de connexion** – **Activer Local Self Help**. Vous pouvez activer ici la fonction à utiliser sur l'ordinateur final et définir d'autres droits et paramètres.

22.1.1 Activation de Local Self Help

Pour activer Local Self Help et l'utiliser sur l'ordinateur final, sélectionnez **Oui** dans le champ **Activer Local Self Help**.

Une fois la stratégie appliquée à l'ordinateur, ce paramètre permet à l'utilisateur d'exploiter Local Self Help pour récupérer la connexion. Pour pouvoir utiliser Local Self Help, l'utilisateur doit alors activer cette méthode de récupération en répondant à un nombre de questions spécifié parmi les questions reçues ou en créant et en répondant à des questions personnalisées (en fonction de ses autorisations).

À cet effet, l'assistant de Local Self Help est disponible via une icône dans la barre des tâches Windows une fois la stratégie appliquée et l'ordinateur redémarré.

22.1.2 Définition de paramètres supplémentaires

Outre l'activation de Local Self Help, vous pouvez définir les paramètres suivants pour cette fonction dans une stratégie du type **Paramètres généraux** :

- **Longueur minimale des réponses**

  Dans ce champ, définissez la longueur minimale (en caractères) des réponses. Le nombre par défaut est **1**.

- **Texte de bienvenue sous Windows**

  Dans ce champ, vous pouvez spécifier le texte d'informations à afficher dans la première boîte de dialogue au démarrage de l'assistant de Local Self Help sur l'ordinateur. Avant de pouvoir spécifier le texte ici, il doit être créé et enregistré.

- **L'utilisateur peut définir des questions personnalisées**

  Les scénarios suivants sont possibles concernant la définition de questions pour Local Self Help :

  - En tant que responsable de la sécurité, définissez les questions et distribuez-les aux utilisateurs. Les utilisateurs ne sont pas autorisés à définir des questions personnalisées.
  - En tant que responsable de la sécurité, définissez les questions et distribuez-les aux utilisateurs. Les utilisateurs sont également autorisés à définir des questions personnalisées. Lorsqu'ils répondent au nombre minimum de questions nécessaire pour activer Local Self Help, les utilisateurs peuvent choisir entre des questions prédéfinies et des questions personnalisées ou une combinaison des deux.

- Vous autorisez les utilisateurs à définir des questions personnalisées. Les utilisateurs activent Local Self Help sur leurs ordinateurs en définissant des questions personnalisées et en y répondant.

Pour autoriser les utilisateurs à définir des questions personnalisées, sélectionnez l'option **Oui** dans le champ **L'utilisateur peut définir des questions personnalisées**.

22.2 Définition de questions

Pour pouvoir utiliser Local Self Help sur un ordinateur final, l'utilisateur doit répondre à dix questions minimum et les enregistrer. Pour se connecter à partir de l'authentification au démarrage via Local Self Help, l'utilisateur doit répondre à cinq questions sélectionnées de façon aléatoire parmi ces dix questions.

Si l'utilisateur n'est pas autorisé à définir des questions personnalisées, vous devez transférer dix questions prédéfinies au minimum vers l'ordinateur au moyen de la stratégie pour permettre à l'utilisateur d'activer Local Self Help.

Pour enregistrer et modifier des questions Local Self Help, en tant que responsable de la sécurité, vous devez disposer du droit **Modifier les questions Local Self Help**.

22.2.1 Utilisation du modèle

Un sujet de question prédéfini est proposé pour Local Self Help. Par défaut, ce sujet de question est disponible en allemand et en anglais sous **Questions Local Self Help** dans la zone de navigation de stratégie.

Le sujet de question est aussi éventuellement disponible en français, italien, espagnol et japonais. Vous pouvez également importer ces versions de langue dans la zone de navigation de stratégie.

Remarque: Lors de la saisie des réponses en japonais pour activer Local Self Help sur les ordinateurs finaux, l'utilisateur doit utiliser les caractères Romaji (Roman). Sinon, les réponses ne correspondent pas lorsque l'utilisateur les saisit dans l'authentification au démarrage.

Vous pouvez utiliser le sujet de question prédéfini tel quel, le modifier ou le supprimer.

Si vous conservez les deux versions de langue du sujet de question prédéfini en l'état et que vous activez Local Self Help à l'aide d'une stratégie du type **Paramètres généraux**, les deux sujets de question prédéfinis sont transférés automatiquement vers l'ordinateur final avec la stratégie.

22.3 Importation de sujets de question

Grâce à la procédure d'importation, vous pouvez importer d'autres versions de langue du sujet de question prédéfini ou de vos listes de questions personnalisées créées sous la forme de fichiers .XML.

Pour importer un ensemble de questions,

1. Créez un sujet de question.
2. Dans la zone de navigation **Stratégies**, sélectionnez le nouveau sujet de question sous **Questions Local Self Help**.
3. Cliquez avec le bouton droit de la souris dans la zone d'action pour ouvrir le menu contextuel du sujet de question. Dans le menu contextuel, sélectionnez **Importer**.
4. Sélectionnez le répertoire et le sujet de question, puis cliquez sur **Ouvrir**.

Les questions importées s'affichent dans la zone d'action. Vous pouvez maintenant enregistrer le sujet de question tel quel ou le modifier.

22.4 Création d'un sujet de question et ajout de questions

Outre l'utilisation de sujets de questions dans différentes langues, vous pouvez également créer de nouveaux sujets de questions portant sur différentes rubriques afin de fournir aux utilisateurs plusieurs sujets de questions différents selon leurs préférences.

Pour créer un sujet de question et ajouter des questions, procédez comme suit :

1. Dans la zone de navigation **Stratégies**, sélectionnez **Questions Local Self Help**.
2. Cliquez avec le bouton droit de la souris sur **Questions Local Self Help**, puis sélectionnez **Nouveau > Sujet de la question**.
3. Saisissez un nom pour le sujet de question et cliquez sur **OK**.
4. Dans la zone de navigation **Stratégies**, sélectionnez le nouveau sujet de question sous **Questions Local Self Help**.
5. Cliquez avec le bouton droit de la souris dans la zone d'action pour ouvrir le menu contextuel du sujet de question. Dans le menu contextuel, sélectionnez **Ajouter**.

6. Une nouvelle ligne de question est ajoutée. Saisissez votre question et appuyez sur **Entrée**. Répétez cette étape pour ajouter d'autres questions.

7. Pour enregistrer vos modifications, cliquez sur l'icône **Enregistrer** dans la barre d'outils.

Votre sujet de question est enregistré et est automatiquement transféré avec la stratégie du type **Paramètres généraux**, activant Local Self Help sur les ordinateurs finaux.

22.5 Modification de sujets de question

Pour modifier des sujets de questions existants, procédez comme suit :

1. Dans la zone de navigation **Stratégies**, sélectionnez le sujet de question souhaité sous **Questions Local Self Help**.

2. Vous pouvez maintenant ajouter, modifier ou supprimer des questions.

   - Pour ajouter des questions, cliquez avec le bouton droit de la souris dans la zone d'action pour afficher le menu contextuel. Dans le menu contextuel, cliquez sur **Ajouter**. Une nouvelle ligne est ajoutée à la liste de questions. Entrez votre question sur la ligne.
   - Pour modifier des questions, cliquez sur le texte de la question souhaitée dans la zone d'action. La question est marquée d'une icône en forme de crayon. Entrez vos modifications sur la ligne de la question.
   - Pour supprimer des questions, sélectionnez la question souhaitée en cliquant sur la case grise située au début de la ligne de la question dans la zone d'action, puis cliquez sur **Supprimer** dans le menu contextuel de la question.

3. Pour enregistrer vos modifications, cliquez sur l'icône **Enregistrer** dans la barre d'outils.

Le sujet de question modifié est enregistré et transféré avec la stratégie du type **Paramètres généraux** qui active Local Self Help sur les ordinateurs finaux.

22.6 Suppression de sujets de question

Pour supprimer intégralement un sujet de question, cliquez avec le bouton droit de la souris sur le sujet concerné **Questions Local Self Help** dans la zone de navigation **Stratégies**, puis sélectionnez **Supprimer**.

Remarque: Si vous supprimez un sujet de question alors que des utilisateurs ont déjà répondu à certaines questions pour activer Local Self Help sur leurs ordinateurs, leurs réponses ne sont plus valides car les questions n'existent plus.

22.7 Enregistrement de textes de bienvenue

Vous pouvez enregistrer un texte de bienvenue à afficher dans la première boîte de dialogue de l'assistant de Local Self Help dans la zone de navigation Stratégies de SafeGuard Management Center.

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans SafeGuard Management Center. La taille maximale de ces fichiers pour les textes d'informations est de 50 Ko. SafeGuard Enterprise n'utilise que des textes codés en Unicode UTF-16. Si vous ne créez pas les fichiers texte dans ce format, ils sont convertis automatiquement lors de l'enregistrement.

Si une conversion s'impose, un message s'affiche et indique que le fichier est en cours de conversion.

Pour enregistrer des textes d'informations :

1. Dans la zone de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Texte d'informations** et sélectionnez **Nouveau > Texte**.
2. Entrez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.
3. Cliquez sur **[...]** pour sélectionner le fichier texte préalablement créé. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Texte d'informations** dans la zone de navigation **Stratégies**. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

23 Récupération via Challenge/Réponse

Pour simplifier le flux de travail et réduire les coûts du support, SafeGuard Enterprise fournit une solution de récupération Challenge/Réponse. SafeGuard Enterprise aide les utilisateurs qui ne parviennent pas à se connecter à leur ordinateur ou qui ne peuvent pas accéder aux données chiffrées en leur proposant un mécanisme de Challenge/Réponse convivial.

Cette fonctionnalité est intégrée à SafeGuard Management Center sous la forme d'un assistant de récupération.

23.1 Avantages de la procédure Challenge/Réponse

Le mécanisme Challenge/Réponse est un système de récupération sécurisé et fiable.

- Tout au long du processus, aucune donnée confidentielle n'est échangée sous une forme autre que chiffrée.
- Cette procédure ne contient aucun point d'écoute électronique de tiers, car les données espionnées ne peuvent pas être utilisées ultérieurement ni sur d'autres périphériques.
- Aucune connexion réseau en ligne n'est nécessaire pour l'ordinateur. L'assistant de code de réponse de Helpdesk s'exécute également sur un ordinateur non géré sans connexion de serveur SafeGuard Enterprise. Aucune infrastructure complexe n'est nécessaire.
- L'utilisateur peut commencer à retravailler rapidement. L'oubli du mot de passe n'entraîne aucune perte de données chiffrées.

23.2 Situations classiques nécessitant l'aide du support

- Un utilisateur a oublié le mot de passe de connexion et l'ordinateur a été verrouillé.
- Le cache local de l'authentification au démarrage est partiellement endommagé.
- Si un utilisateur est absent, ses collègues doivent pouvoir accéder aux données de son ordinateur.
- Un utilisateur souhaite accéder à un volume chiffré à l'aide d'une clé qui n'est pas disponible sur l'ordinateur.

SafeGuard Enterprise propose différents flux de travail de récupération pour ces scénarios classiques, ce qui permet aux utilisateurs d'accéder de nouveau à leur ordinateur.

23.3 Flux de travail de challenge/réponse

La procédure Challenge/Réponse repose sur les deux composants suivants :

- l'ordinateur final sur lequel le code de challenge sera généré ;
- SafeGuard Management Center où, en tant que responsable du support possédant les droits correspondants, vous créerez un code de réponse qui autorisera l'utilisateur à effectuer l'action requise sur l'ordinateur.

1. Sur l'ordinateur final, l'utilisateur demande le code de challenge. En fonction du type de récupération, cette opération s'effectue soit dans l'authentification au démarrage, soit via l'outil de récupération de clé KeyRecovery.

Un code de challenge sous la forme d'une chaîne de caractères ASCII est généré et s'affiche.

2. L'utilisateur contacte le support. Il lui fournit les données d'identification nécessaires, ainsi que le code de challenge.
3. Le support lance l'assistant de récupération dans SafeGuard Management Center.
4. Le support sélectionne le type de récupération approprié, confirme les données d'identification et le code de challenge, puis sélectionne l'action de récupération souhaitée.

Un code de réponse sous la forme d'une chaîne de caractères ASCII est généré et s'affiche.

5. Le support transmet le code de réponse à l'utilisateur, par exemple par téléphone ou message texte.
6. L'utilisateur saisit le code de réponse, En fonction du type de récupération, cette opération s'effectue soit dans l'authentification au démarrage, soit via l'outil de récupération de clé KeyRecovery.

L'utilisateur est ensuite autorisé à effectuer l'action convenue, par exemple à réinitialiser le mot de passe et à reprendre son travail.

23.4 Exigences liées au changement du mot de passe de l'utilisateur

Dans le cadre du processus de récupération de SafeGuard Enterprise, l'utilisateur peut être contraint de changer son mot de passe Windows. Le tableau suivant fournit des informations sur les cas dans lesquels un changement de mot de passe est requis. Les quatre premières colonnes indiquent les conditions spécifiques pouvant se produire lors de la procédure Challenge/Réponse.

La dernière colonne indique si l'utilisateur est contraint de changer son mot de passe Windows, en fonction des conditions indiquées dans les colonnes précédentes.

Condition : procédure C/R générée avec connexion de l'utilisateur et option d'affichage du mot de passe	Condition : procédure C/R générée avec connexion de l'utilisateur	Condition : contrôleur de domaine disponible	Condition : affichage du mot de passe refusé par l'utilisateur	Résultat : l'utilisateur est contraint de changer son mot de passe Windows
Oui	Oui	Oui	Non	**Non**
Oui	Oui	Oui	Oui	**Oui**
Oui	Oui	Non	Oui	**Non**
Non	Oui	Oui	Non disponible	**Oui**
Non	Oui	Non	Non disponible	**Non**
Non	Non	Non	Non disponible	**Non**

23.5 Ouverture de l'assistant de récupération

Pour pouvoir effectuer une procédure de récupération, assurez-vous de disposer des droits et des autorisations requis.

1. Connectez-vous à SafeGuard Management Center.
2. Cliquez sur **Outils > Récupération** dans la barre de menus.

L'assistant de récupération SafeGuard démarre. Vous pouvez sélectionner le type de récupération demandé.

23.6 Types de récupération

Sélectionnez le type de récupération que vous souhaitez utiliser. Les types de récupération suivants sont fournis :

- **Procédure Challenge/Réponse pour clients SafeGuard Enterprise (gérés)**

  Procédure Challenge/Réponse pour ordinateurs gérés de façon centralisée par SafeGuard Management Center. Ces ordinateurs sont répertoriés dans la zone **Utilisateurs & ordinateurs** de SafeGuard Management Center.

- **Challenge/Réponse à l'aide de clients virtuels**

  Les volumes chiffrés peuvent être récupérés facilement grâce à des fichiers spécifiques appelés clients virtuels, dans les cas où la procédure Challenge/Réponse n'est pas prise en charge, par exemple lorsque l'authentification au démarrage est corrompue.

- **Procédure Challenge/Réponse pour clients Sophos SafeGuard (autonomes)**

  Procédure Challenge/Réponse pour ordinateurs gérés localement. Ils ne sont jamais connectés au serveur SafeGuard Enterprise. Pour chaque ordinateur géré localement, un fichier de récupération de clé est généré au cours de la configuration. Il contient la clé machine définie, qui est chiffrée avec le certificat de l'entreprise. Si ce fichier de clés de récupération est disponible, par exemple sur une carte mémoire ou via un chemin réseau partagé afin que le responsable support puisse y accéder, la procédure Challenge/Réponse pour un ordinateur autonome est prise en charge.

Remarque: Par ailleurs, la méthode de récupération de connexion Local Self Help ne requiert aucune assistance du support.

23.7 Récupération via la procédure Challenge/Réponse pour des clients SafeGuard Enterprise

SafeGuard Enterprise fournit la procédure de récupération relative à différents scénarios d'urgence pour les ordinateurs finaux protégés par SafeGuard Enterprise et enregistrés dans la base de données, par exemple la récupération de mots de passe ou l'accès aux données via l'amorçage à partir d'un support externe.

La procédure challenge/réponse est prise en charge pour les ordinateurs natifs SafeGuard Enterprise et les ordinateurs finaux chiffrés BitLocker. Lors de cette procédure, le système détermine, de façon dynamique, le type d'ordinateur utilisé et le flux de travail de récupération est réglé en conséquence.

23.7.1 Actions de récupération pour les clients SafeGuard Enterprise

Le flux de travail de récupération dépend du type d'ordinateur final pour lequel une récupération est demandée.

Avis : s'il s'agit d'ordinateurs chiffrés BitLocker, la seule action de récupération consiste à récupérer la clé utilisée pour chiffrer un volume spécifique. La récupération de mots de passe n'est pas proposée.

23.7.1.1 Récupération du mot de passe au niveau de l'authentification au démarrage

L'un des scénarios les plus courants est l'oubli du mot de passe par l'utilisateur. Par défaut, SafeGuard Enterprise est installé avec l'authentification au démarrage (POA) activée. Le mot de passe POA permettant d'accéder à l'ordinateur est identique au mot de passe Windows.

Si l'utilisateur a oublié le mot de passe au niveau de l'authentification au démarrage, le responsable support SafeGuard Enterprise génère une réponse pour **Initialiser le client SGN avec une connexion utilisateur**, mais sans afficher le mot de passe utilisateur. Toutefois, dans ce cas, après avoir saisi le code de réponse, l'ordinateur amorce le système d'exploitation. L'utilisateur doit donc changer le mot de passe au niveau de Windows à condition que le domaine soit accessible. L'utilisateur peut alors se connecter à Windows ainsi qu'à l'authentification au démarrage à l'aide du nouveau mot de passe.

Pratique recommandée pour la récupération du mot de passe au niveau POA

Avis : nous recommandons d'utiliser en priorité les méthodes suivantes lorsque l'utilisateur a oublié son mot de passe afin d'éviter que ce dernier ne soit réinitialisé de manière centralisée :

Utiliser Local Self Help. Avec la récupération via Local Self Help, l'utilisateur peut afficher le mot de passe actuel et continuer à l'utiliser sans avoir à le réinitialiser et donc sans l'aide du support. Pour plus d'informations, voir *Options de récupération* en page 231.

Avec Challenge/Réponse. Nous recommandons d'éviter la réinitialisation centralisée du mot de passe dans Active Directory avant la procédure Challenge/Réponse. Vous vous assurez ainsi que le mot de passe reste synchronisé entre Windows et SafeGuard Enterprise. Vérifiez que le support Windows dispose de l'instruction adéquate.

En tant que responsable support SafeGuard Enterprise, générez une réponse pour **Initialiser le client SGN avec une connexion utilisateur** avec l'option **Afficher le mot de passe utilisateur**. Cette méthode est avantageuse dans le sens où il n'est pas nécessaire de réinitialiser le mot de passe dans Active Directory. L'utilisateur peut continuer à travailler avec l'ancien mot de passe et le modifier en local ultérieurement, s'il le souhaite.

23.7.1.2 Affichage du mot de passe utilisateur

SafeGuard Enterprise permet aux utilisateurs d'afficher leur mot de passe lors de la procédure challenge/réponse. Ainsi, ils ne sont pas tenus de réinitialiser le mot de passe dans Active Directory. Cette option est disponible uniquement si l'**Initialisation du client SGN avec une connexion utilisateur** est demandée.

23.7.1.3 Amorçage de l'ordinateur protégé par SafeGuard Enterprise par un autre utilisateur

Dans ce cas, l'utilisateur devant accéder à l'ordinateur amorce l'ordinateur et saisit son nom d'utilisateur. L'utilisateur demande ensuite un challenge. Le support SafeGuard génère une réponse du type **Initialiser le client SGN sans connexion utilisateur**, avec l'option **Authentification automatique à Windows** activée. L'utilisateur est connecté et peut utiliser l'ordinateur.

23.7.1.4 Accès aux données via l'initialisation à partir d'un support externe

Il est également possible d'utiliser la procédure challenge/réponse pour autoriser la réinitialisation d'un ordinateur à partir d'un support externe, par exemple WinPE. Pour ce faire, l'utilisateur doit sélectionner **Poursuivre l'initialisation à partir de : Disquette/Support externe** dans la boîte de dialogue de connexion de l'authentification au démarrage et initier le challenge. Lors de la réception de la réponse, l'utilisateur peut saisir les informations d'identification dans POA, de façon habituelle, et poursuivre l'initialisation à partir d'un support externe.

Les conditions suivantes doivent être remplies pour que vous puissiez accéder à un volume chiffré :

- Le périphérique à utiliser doit contenir le pilote du filtre SafeGuard Enterprise. Une description détaillée de la création d'un CD de pilote de ce type est indiquée dans notre base de connaissances (en anglais) :

  http://www.sophos.com/support/knowledgebase/article/108805.html.

- L'utilisateur doit amorcer à partir du support externe et doit disposer de l'autorisation appropriée. Ce droit peut être octroyé à l'utilisateur en définissant une stratégie dans SafeGuard Management Center et en l'affectant à l'ordinateur : (type de stratégie Authentification > Accès : L'utilisateur peut uniquement bouter à partir du disque dur doit être définie sur Non). Par défaut, le droit d'initialisation à partir d'un support externe n'est pas affecté.
- En général, l'ordinateur final doit prendre en charge l'initialisation à partir de supports autres qu'un disque dur fixe.
- Seuls les volumes chiffrés avec la clé machine définie sont accessibles. Ce type de chiffrement de clés peut être défini dans une stratégie de chiffrement du périphérique dans SafeGuard Management Center et attribué à l'ordinateur.

Notez que l'utilisation de supports externes, par exemple WinPE, pour accéder à un lecteur chiffré autorise uniquement un accès partiel au volume.

23.7.1.5 Restauration du cache de stratégies SafeGuard Enterprise

Cette procédure est nécessaire si le cache de stratégies SafeGuard est endommagé. Le cache local stocke la totalité des clés, stratégies, certificats utilisateur et fichiers d'audit. La récupération de connexion est désactivée par défaut lorsque le cache local est corrompu, c'est-à-dire qu'il est restauré automatiquement à partir de sa sauvegarde. Aucune procédure de Challenge/Réponse n'est donc requise pour réparer le cache local. Toutefois, la récupération de la connexion peut être activée par stratégie, si le cache local doit être réparé explicitement par une procédure Challenge/Réponse. Dans ce cas, l'utilisateur est invité automatiquement à démarrer une procédure Challenge/Réponse si le cache local est corrompu.

23.7.2 Réponse pour les clients SafeGuard Enterprise

Pour générer une réponse lors de la procédure challenge/réponse pour un client SafeGuard Enterprise, les noms de l'ordinateur final et du domaine sont requis.

Avis : ce nom doit toujours correspondre au nom unique de l'ordinateur.

1. Dans la fenêtre **Type de récupération**, sélectionnez **Client SafeGuard Enterprise** (**géré**).
2. Dans la liste, sélectionnez le domaine requis.
3. Saisissez le nom de l'ordinateur requis. Pour ce faire, vous pouvez procéder de plusieurs façons :
   - Sélectionnez un nom en cliquant sur [**...**] dans la section **Informations ordinateur** de la boîte de dialogue **Type de récupération**. Cliquez alors sur **Rechercher maintenant**. La liste des ordinateurs s'affiche. Sélectionnez l'ordinateur requis, puis cliquez sur **OK**. Le nom de l'ordinateur s'affiche maintenant dans la fenêtre **Type de récupération** sous **Domaine**.

- Saisissez le nom abrégé de l'ordinateur. Lorsque vous cliquez sur **Suivant**, ce nom est recherché dans la base de données. S'il est trouvé, le nom d'ordinateur unique s'affiche.
- Saisissez directement le nom de l'ordinateur au format de nom unique, par exemple :

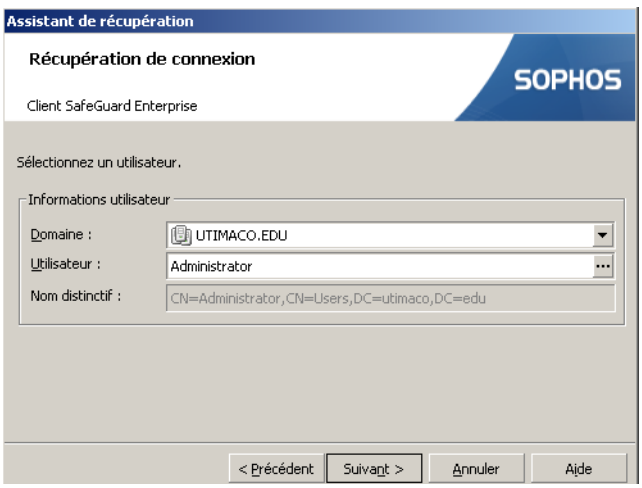
  `CN=Poste1,OU=Développement,OU=Siège,DC=Sophos,DC=edu`

4. Cliquez sur **Suivant**.

Le programme détermine alors de façon dynamique si un ordinateur SafeGuard Enterprise natif ou si un ordinateur chiffré BitLocker est utilisé et règle le flux de travail de récupération en conséquence. S'il s'agit d'un ordinateur SafeGuard Enterprise natif, l'étape suivante requiert la sélection des informations utilisateur.

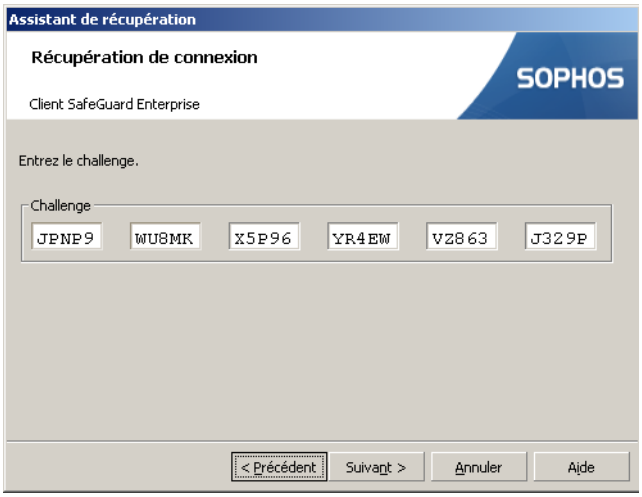
Une fois terminée la recherche de l'ordinateur approprié dans la base de données, le nom d'utilisateur et le domaine correspondants sont requis afin d'effectuer la récupération d'un client SafeGuard Enterprise.

1. Sélectionnez le domaine requis de l'utilisateur.
2. Saisissez le nom de l'utilisateur requis. Pour ce faire, vous pouvez procéder de plusieurs façons :
   - Sélectionnez un nom en cliquant sur [**...**] dans la section **Informations utilisateur** de la boîte de dialogue **Récupération de connexion**. Cliquez alors sur **Rechercher maintenant**. La liste des utilisateurs s'affiche. Sélectionnez le nom requis, puis cliquez sur **OK**. Le nom s'affiche maintenant dans la fenêtre **Type de récupération** sous **Domaine**.
   - Saisissez directement le nom de l'utilisateur. Assurez-vous de l'orthographier correctement.

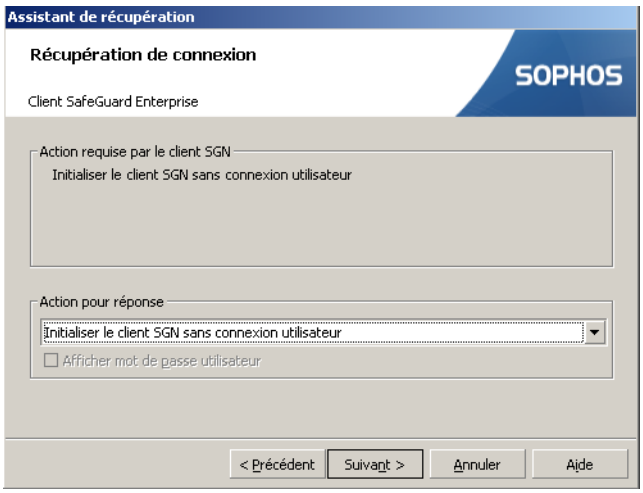


3. Cliquez sur **Suivant**. Une fenêtre s'affiche, dans laquelle vous pouvez saisir le code de challenge.

4. Saisissez le code de challenge que l'utilisateur vous a indiqué, puis cliquez sur **Suivant**. Ce code est vérifié. S'il a été saisi de façon incorrecte, le terme `Non valide` s'affiche au-dessous du bloc contenant l'erreur.



5. Si le code de challenge a été saisi correctement, l'action de récupération demandée par le client SafeGuard Enterprise, ainsi que les actions de récupération possibles sur ce client s'affichent. Les actions possibles pour la réponse dépendent des actions demandées côté client lors de l'appel du challenge. Par exemple, si l'action **Carte à puce crypto requise** est requise côté client, les actions disponibles pour la réponse sont **Initialiser le client SGN avec une connexion utilisateur** et **Initialiser le client SGN sans connexion utilisateur**.

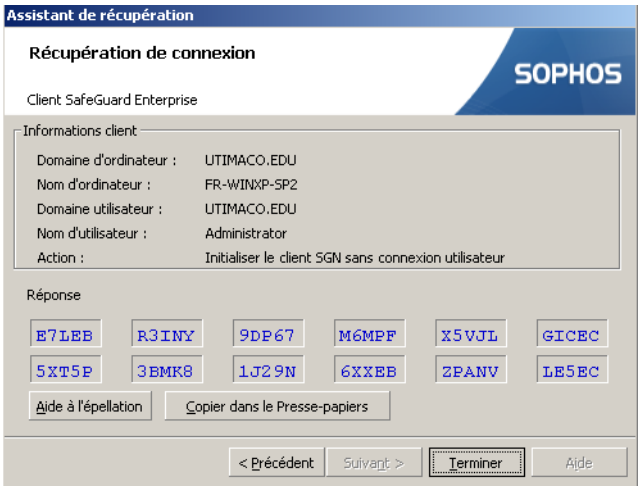


6. Sélectionnez l'action que l'utilisateur doit exécuter.

7. Si l'action **Initialisation du client SGN avec une connexion utilisateur** a été sélectionnée comme réponse, vous pouvez également sélectionner **Afficher le mot de passe utilisateur** afin d'afficher le mot de passe sur l'ordinateur cible.

8. Cliquez sur **Suivant**.

9. Un code de réponse est généré. Lisez-le à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.



L'utilisateur peut ensuite saisir le code de réponse sur l'ordinateur final et exécuter l'action autorisée.

23.8 Réponse pour les clients SafeGuard Enterprise chiffrés BitLocker

S'il s'agit d'ordinateurs chiffrés BitLocker, un volume qui n'est plus accessible peut être récupéré.

Pour générer une réponse lors de la procédure challenge/réponse pour un client SafeGuard Enterprise, les noms de l'ordinateur final et du domaine sont requis.

Avis : ce nom doit toujours correspondre au nom unique de l'ordinateur.

1. Dans la fenêtre **Type de récupération**, sélectionnez **Client SafeGuard Enterprise**.
2. Dans la liste, sélectionnez le domaine requis.
3. Saisissez le nom de l'ordinateur requis. Pour ce faire, vous pouvez procéder de plusieurs façons :
   - Sélectionnez un nom en cliquant sur [**...**] dans la section **Informations ordinateur** de la boîte de dialogue **Type de récupération**. Cliquez alors sur **Rechercher maintenant**. La liste des ordinateurs s'affiche. Sélectionnez l'ordinateur requis, puis cliquez sur **OK**. Le nom de l'ordinateur s'affiche alors dans la fenêtre **Type de récupération** sous **Domaine**.
   - Saisissez le nom abrégé de l'ordinateur. Lorsque vous cliquez sur **Suivant**, ce nom est recherché dans la base de données. S'il est trouvé, le nom d'ordinateur unique s'affiche.
   - Saisissez directement le nom de l'ordinateur au format de nom unique, par exemple :
   - `CN=Poste1,OU=Développement,OU=Siège,DC=Utimaco,DC=uae`
4. Cliquez sur **Suivant**.

Le programme détermine alors de façon dynamique si un ordinateur SafeGuard Enterprise natif ou si un ordinateur chiffré BitLocker est utilisé et règle le flux de travail de récupération en conséquence. S'il s'agit d'un ordinateur chiffré BitLocker, l'étape suivante nécessite la sélection du volume requis.

Une fois terminée la recherche de l'ordinateur approprié dans la base de données, le volume requis est nécessaire à la récupération d'un ordinateur final chiffré BitLocker.

1. Dans la liste, sélectionnez le volume auquel accéder, puis cliquez sur **Suivant**.
2. L'assistant de récupération affiche alors la clé de récupération à 48 chiffres correspondante.
3. Lisez cette clé à l'utilisateur.

L'utilisateur peut alors la saisir afin de récupérer le volume chiffré BitLocker sur l'ordinateur final.

23.9 Récupération via la procédure Challenge/Réponse à l'aide de clients virtuels

Grâce à la récupération des clients virtuels, SafeGuard Enterprise permet de récupérer des volumes chiffrés même dans des situations d'urgence complexes, par exemple lorsque l'authentification au démarrage est corrompue. La récupération des clients virtuels s'applique aussi bien aux clients virtuels qu'aux ordinateurs autonomes.

Remarque: La récupération des clients virtuels doit uniquement être utilisée pour résoudre des situations d'urgence complexes. Si, par exemple, une seule clé manque pour la récupération d'un volume, la meilleure solution consiste à affecter tout simplement la clé manquante au jeu de clés de l'utilisateur approprié.

23.9.1 Flux de travail de récupération à l'aide de clients virtuels

Pour accéder à l'ordinateur chiffré, voici le flux de travail général qui s'applique :

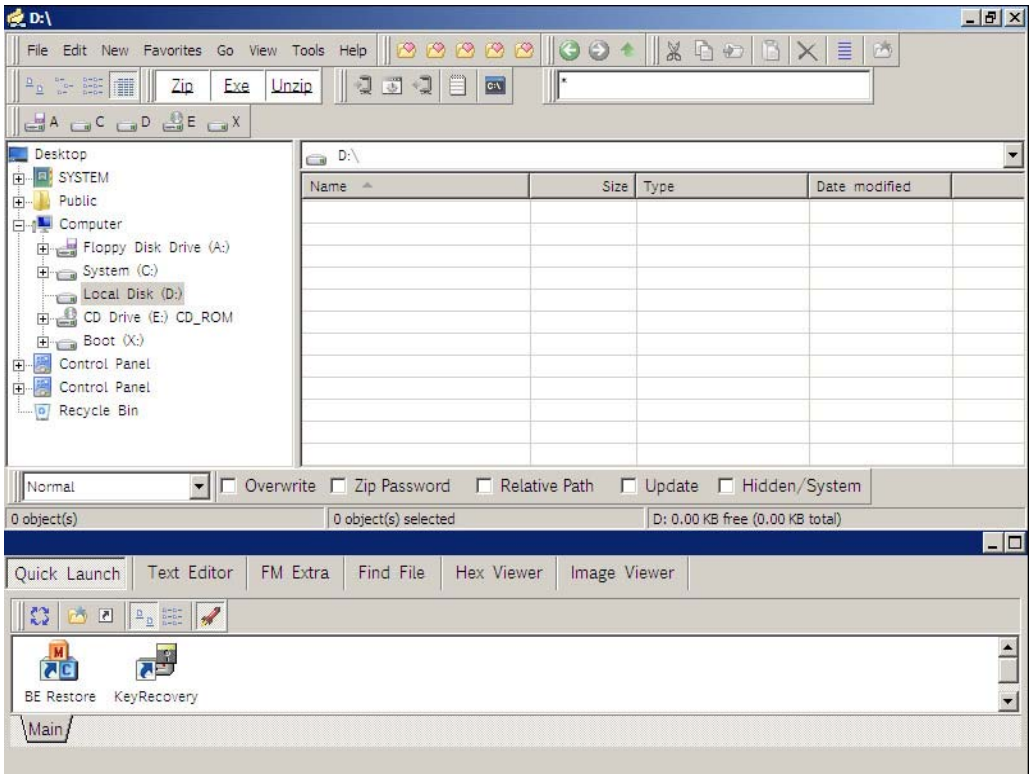
1. Demandez au support technique de vous fournir le disque de récupération SafeGuard Enterprise.
2. Le support peut télécharger le disque de récupération Windows PE avec les derniers pilotes du filtre SafeGuard Enterprise le site du support Sophos. Pour en savoir plus, consultez la base de connaissances : http://www.sophos.com/support/knowledgebase/article/108805.html.
3. Créez le client virtuel dans SafeGuard Management Center.
4. Exportez le client virtuel dans un fichier.
5. Démarrez l'ordinateur depuis le disque de récupération.
6. Importez le fichier du client virtuel dans l'outil de récupération de clé KeyRecovery.
7. Initialisez le challenge dans l'outil de récupération de clé KeyRecovery.
8. Confirmez le client virtuel dans SafeGuard Management Center.
9. Sélectionnez l'action de récupération requise.
10. Saisissez le code de challenge dans SafeGuard Management Center.
11. Générez le code de réponse dans SafeGuard Management Center.
12. Saisissez le code de réponse dans l'outil de récupération de clé KeyRecovery.

L'ordinateur est accessible à nouveau.

23.9.2 Initialisation de l'ordinateur depuis le disque de récupération

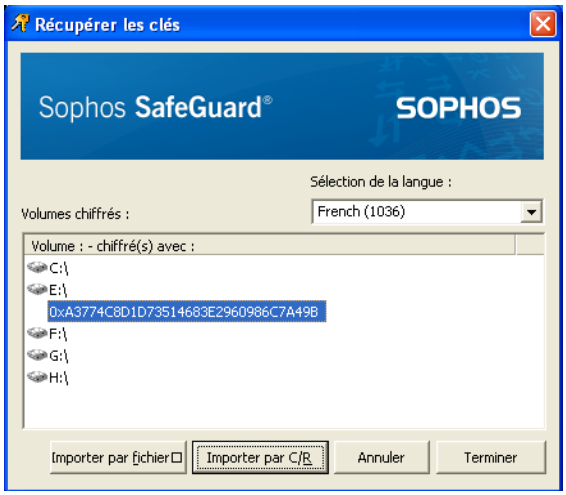
Vérifiez que la séquence d'initialisation dans les paramètres du BIOS permet de démarrer à partir du CD.

1. Insérez le disque de récupération, puis démarrez l'ordinateur final. Le gestionnaire de fichiers intégré s'ouvre. Les volumes et les lecteurs présents s'affichent immédiatement.



Le contenu du lecteur chiffré ne s'affiche pas dans le gestionnaire de fichiers. Ni le système de fichiers, ni la capacité et l'espace utilisé/libre ne figurent dans les propriétés du lecteur chiffré.

2. Au bas du gestionnaire de fichiers, dans la section **Lancement rapide**, cliquez sur l'icône KeyRecovery pour ouvrir l'outil de récupération de clé KeyRecovery. L'outil de récupération de clé KeyRecovery affiche les ID de clé des lecteurs chiffrés.



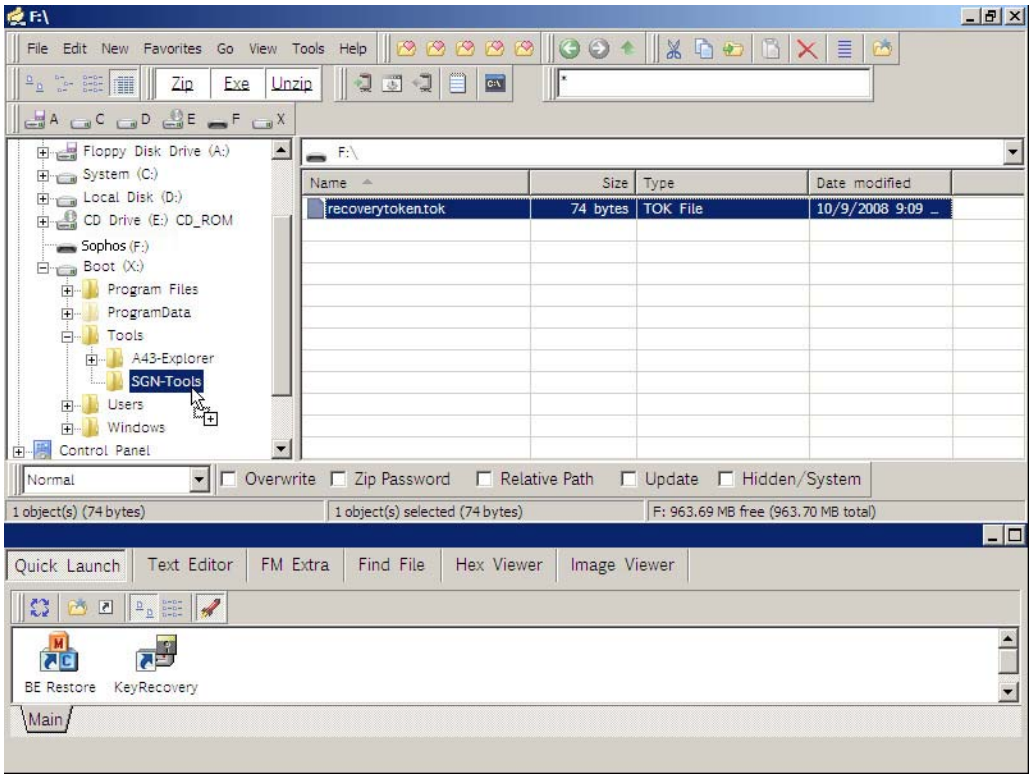
3. Recherchez les ID de clé des lecteurs auxquels vous souhaitez accéder. Vous devrez fournir cet ID de clé ultérieurement.

Importez ensuite le client virtuel dans l'outil de récupération de clé.

23.9.3 Importation du client virtuel dans l'outil de récupération de clé KeyRecovery

- L'ordinateur a été initialisé depuis le disque de récupération.
- Vérifiez que le lecteur USB, sur lequel est enregistré le fichier du client virtuel recoverytoken.tok, a été correctement monté.

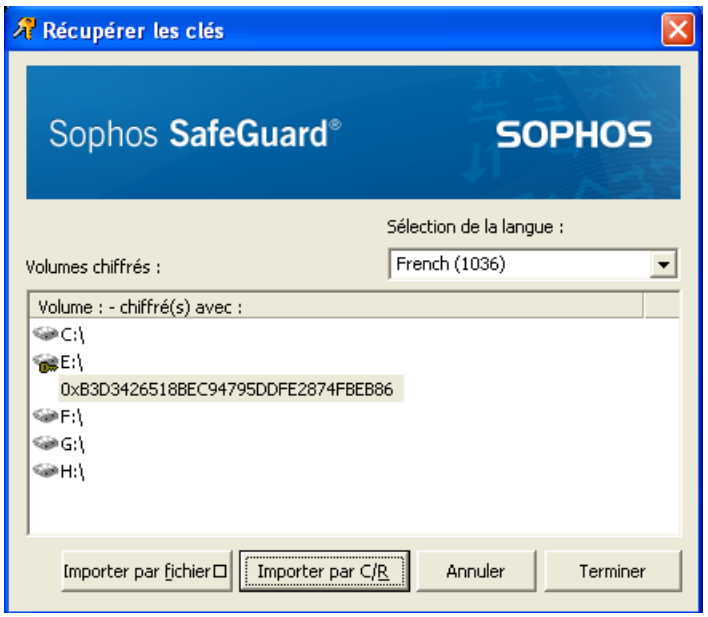
1. Dans le gestionnaire de fichiers Windows PE, sélectionnez le lecteur sur lequel est enregistré le client virtuel. Le fichier recoverytoken.tok s'affiche sur la droite.
2. Sélectionnez le fichier recoverytoken.tok et faites-le glisser sur le lecteur où se trouve l'outil de récupération de clé KeyRecovery. Déposez-le dans le répertoire Outils\Outils-SGN.



23.9.4 Lancement d'une procédure Challenge dans l'outil Recover Keys

1. Au bas du gestionnaire de fichiers Windows PE, dans la section **Lancement rapide**, cliquez sur l'icône KeyRecovery pour ouvrir l'outil de récupération de clé KeyRecovery. L'outil de récupération de clé KeyRecovery affiche les ID de clé des lecteurs chiffrés.

Cet outil démarre et affiche une liste de tous les volumes, ainsi que des informations de chiffrement correspondantes (ID de clé).



2. Sélectionnez le volume à déchiffrer, puis cliquez sur Importer par C/R pour générer le code de challenge.

À titre de référence dans la base de données SafeGuard Enterprise, le fichier client virtuel est utilisé et mentionné dans la procédure Challenge. Le code de challenge est alors généré et s'affiche.

3. Communiquez le nom du client virtuel et le code de challenge au support, par exemple par téléphone ou en envoyant un message texte. Une aide à l'épellation est fournie.

23.9.5 Génération d'une réponse à l'aide de clients virtuels

Pour accéder à un ordinateur protégé par SafeGuard Enterprise et générer une réponse à l'aide de clients virtuels, deux actions sont requises :

1. Confirmez le client virtuel dans la base de données de SafeGuard Management Center.
2. Sélectionnez l'action de récupération requise :
   - Un challenge peut être initié pour récupérer une seule clé afin d'accéder à un volume chiffré sur un ordinateur connecté au serveur SafeGuard Enterprise. Sélectionnez la clé de récupération **Clé requise à partir de la base de données.**
   - Un challenge peut être initié pour récupérer une seule clé afin d'accéder à un volume chiffré sur un ordinateur autonome jamais connecté au serveur SafeGuard Enterprise. Sélectionnez le fichier de récupération de clé (autonome) **Clé requise.**
   - Un challenge peut être initié pour récupérer plusieurs clés afin d'accéder à des volumes chiffrés sur un ordinateur connecté au serveur SafeGuard Enterprise. Les clés sont stockées dans un fichier, chiffré par un mot de passe aléatoire enregistré dans la base de données. Ce mot de passe est propre à chaque fichier de clés créé. Le mot de passe figurant dans le code de réponse est transféré sur l'ordinateur cible. Sélectionnez **Fichier de clés requis**.

23.9.6 Confirmation du client virtuel

Le client virtuel doit avoir été créé dans SafeGuard Management Center sous **Clients virtuels** ainsi qu'être disponible dans la base de données.

1. Dans SafeGuard Management Center, cliquez sur **Outils > Récupération** pour ouvrir l'assistant de récupération.
2. Dans **Type de récupération**, sélectionnez **Client virtuel**.
3. Saisissez le nom du client virtuel que l'utilisateur vous a indiqué. Pour ce faire, vous pouvez procéder de plusieurs façons :
   - Saisissez directement le nom unique.
   - Sélectionnez un nom en cliquant sur **[...]** dans la section **Client virtuel** de la boîte de dialogue **Type de récupération**. Cliquez ensuite sur **Rechercher maintenant**. La liste des clients virtuels s'affiche. Sélectionnez le client virtuel requis, puis cliquez sur **OK**. Le nom du client virtuel s'affiche alors dans la fenêtre **Type de récupération** sous **Client virtuel**.

4. Cliquez sur **Suivant** pour confirmer le nom du fichier du client virtuel.

Ensuite, sélectionnez l'action de récupération requise.

23.9.7 Sélection de la clé requise (clients gérés)

Sélectionnez au préalable le client virtuel requis dans l'assistant de récupération SafeGuard Management Center.

Une réponse ne peut être initiée que pour des clés attribuées. Si une clé est inactive, à savoir qu'elle n'est pas attribuée à un utilisateur au moins, une réponse pour client virtuel est impossible. Dans ce cas, la clé inactive peut être réattribuée à un autre utilisateur et une réponse pour cette clé peut être de nouveau générée.

1. Dans l'assistant de récupération, dans le client virtuel, sélectionnez l'action de récupération **Clé requise**, puis cliquez sur **Suivant**.
2. Activez **Sélectionner la clé de récupération à partir de la base de données**.
3. Cliquez sur **[...]**. Vous pouvez afficher les clés en fonction de leur ID ou de leur nom symbolique. Cliquez sur **Rechercher**, sélectionnez la clé, puis cliquez sur **OK**.
4. Cliquez sur **Suivant** pour confirmer. La fenêtre dans laquelle vous devez saisir le code de challenge s'affiche.
5. Saisissez le code de challenge que l'utilisateur vous a indiqué, puis cliquez sur **Suivant**. Ce code est vérifié.

Si le code de challenge a été saisi correctement, le code de réponse est généré. S'il a été saisi de façon incorrecte, le terme **Non valide** s'affiche au-dessous du bloc contenant l'erreur.

6. Lisez alors le code de réponse à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

La clé requise est transférée vers l'environnement de l'utilisateur, dans le code de réponse.

23.9.8 Sélection du fichier de récupération de clé (ordinateur autonome)

Sélectionnez au préalable le client virtuel requis dans l'assistant de récupération SafeGuard Management Center.

Le support doit pouvoir accéder au fichier de récupération de clé nécessaire pour récupérer l'accès à l'ordinateur. Ce fichier peut par exemple se trouver sur un partage réseau

1. Dans l'assistant de récupération, dans le client virtuel, sélectionnez l'action de récupération **Clé requise**, puis cliquez sur **Suivant**.
2. Activez l'option **Sélectionner un fichier de récupération de clé contenant une clé de récupération**.
3. Cliquez sur **[...]** en regard de cette option pour rechercher le fichier. Pour faciliter l'identification des fichiers de récupération, leur nom est identique à celui de l'ordinateur : nomordinateur.GUID.xml.
4. Cliquez sur **Suivant** pour confirmer. La fenêtre dans laquelle vous devez saisir le code de challenge s'affiche.
5. Saisissez le code de challenge que l'utilisateur vous a indiqué, puis cliquez sur **Suivant**. Ce code est vérifié.

Si le code de challenge a été saisi correctement, le code de réponse est généré. S'il a été saisi de façon incorrecte, le terme **Non valide** s'affiche au-dessous du bloc contenant l'erreur.

6. Lisez alors le code de réponse à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

La clé requise est transférée vers l'environnement de l'utilisateur, dans le code de réponse.

23.9.9 Sélection de plusieurs clés dans un fichier de clés

Sélectionnez au préalable le client virtuel requis dans l'assistant de récupération SafeGuard Management Center.

Sélectionnez au préalable le fichier de clés dans SafeGuard Management Center, sous **Clés et certificats**. En outre, le mot de passe de chiffrement du fichier de clés doit être stocké dans la base de données.

1. Dans l'assistant de récupération, dans le client virtuel, sélectionnez l'action de récupération **Mot de passe du fichier de clés requis**, puis cliquez sur **Suivant**.
2. Cliquez sur **[...]** en regard de cette option, puis sur **Rechercher**. Sélectionnez le fichier de clés, puis cliquez sur **OK**.
3. Cliquez sur **Suivant** pour confirmer. La fenêtre dans laquelle vous devez saisir le code de challenge s'affiche.
4. Saisissez le code de challenge que l'utilisateur vous a indiqué, puis cliquez sur **Suivant**. Ce code est vérifié.

Si le code de challenge a été saisi correctement, le code de réponse est généré. S'il a été saisi de façon incorrecte, le terme **Non valide** s'affiche au-dessous du bloc contenant l'erreur.

5. Lisez alors le code de réponse à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

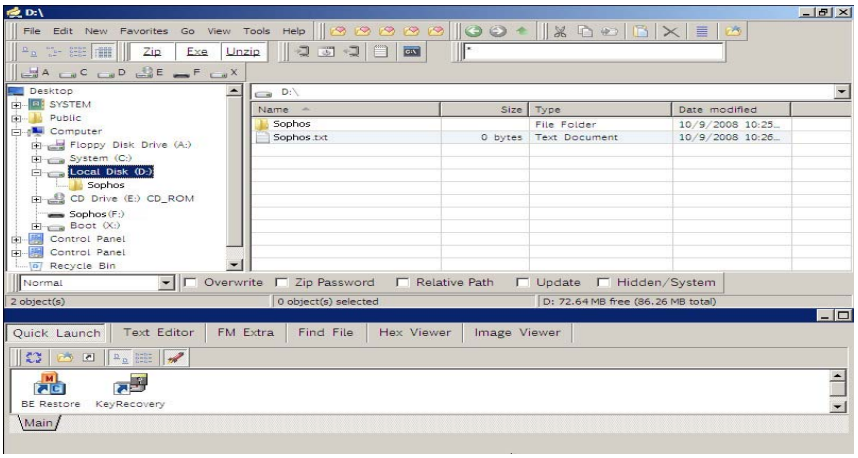
Le mot de passe du fichier de clés chiffré est transféré dans le code de réponse. Ce fichier de clés est ensuite supprimé.

23.9.10 Saisie du code de réponse dans l'outil de récupération de clé KeyRecovery

1. Sur l'ordinateur final, dans l'outil de récupération de clé KeyRecovery, entrez le code de réponse fourni par le support.

   La clé ou le mot de passe requis pour le fichier de clés figure dans ce code de réponse.
2. Cliquez sur OK. Le disque sélectionné pour la procédure Challenge/Réponse a été déchiffré.

3. Pour vérifier si le déchiffrement a réussi, sélectionnez le lecteur déchiffré dans le gestionnaire de fichiers Windows PE :



Le contenu du lecteur déchiffré s'affiche dans le gestionnaire de fichiers. Le système de fichiers, ainsi que la capacité et l'espace utilisé/libre, figurent dans les propriétés du lecteur déchiffré.

L'accès aux données stockées sur cette partition est récupéré. Suite à ce déchiffrement réussi, vous pouvez lire, écrire et copier des données à partir du disque indiqué et/ou vers celui-ci.

23.10 Procédure Challenge/Réponse pour clients Sophos SafeGuard (autonomes)

SafeGuard Enterprise inclut également des procédures Challenge/Réponse pour les ordinateurs non gérés (clients Sophos SafeGuard). Ces ordinateurs ne disposent d'aucune connexion, même temporaire, au serveur SafeGuard Enterprise. Ils fonctionnent en mode autonome. Comme ils ne sont pas enregistrés dans la base de données SafeGuard Enterprise, aucune information sur leur identification nécessaire à une procédure challenge/réponse n'est disponible.

Pour ces ordinateurs, SafeGuard Enterprise propose une procédure Challenge/Réponse, par exemple si l'utilisateur a oublié son mot de passe ou s'il l'a saisi de manière incorrecte un trop grand nombre de fois. Dans ce cas, les informations d'identification nécessaires à la procédure Challenge/Réponse sont basées sur le fichier de récupération des clés.

Sur chaque ordinateur final, un fichier de récupération des clés est généré lors de l'installation du logiciel de chiffrement SafeGuard Enterprise. Il contient la clé machine définie, qui est chiffrée avec le certificat de l'entreprise.

Si ce fichier de récupération des clés est accessible au support, par exemple par l'intermédiaire d'un chemin réseau partagé, une procédure Challenge/Réponse pour un ordinateur protégé par SafeGuard Enterprise peut être fournie.

Afin de faciliter la recherche et le regroupement des fichiers de récupération, ils portent le nom de l'ordinateur : nomordinateur.GUID.xml. Vous pouvez ainsi effectuer des recherches de caractères génériques avec des astérisques (*), par exemple : *.GUID.xml.

Remarque: Lorsqu'un ordinateur est renommé, le cache local de l'ordinateur n'applique pas ce changement de nom. Afin de permettre la génération du fichier, le nom de l'ordinateur doit donc être supprimé du cache local mais restera le même, bien que l'ordinateur ait été renommé sous Windows.

23.10.1 Actions de récupération pour les clients Sophos SafeGuard (autonomes)

La procédure Challenge/Réponse pour un ordinateur final intervient dans les situations suivantes :

- L'utilisateur a saisi trop fréquemment le mot de passe de façon incorrecte.
- L'utilisateur a oublié le mot de passe.
- Un cache endommagé doit être réparé.

Aucune clé utilisateur n'est disponible dans la base de données pour un ordinateur non géré. Par conséquent, la seule action de récupération possible dans une session de Challenge/Réponse est **Initialisation du client SGN sans connexion utilisateur**.

La procédure Challenge/Réponse permettra à l'utilisateur de se connecter à partir de l'authentification au démarrage. L'utilisateur pourra également se connecter à Windows.

L'utilisateur a saisi trop fréquemment le mot de passe de façon incorrecte

Comme dans ce cas, la réinitialisation du mot de passe n'est pas nécessaire, la procédure Challenge/Réponse permet à l'utilisateur de se connecter à l'authentification au démarrage. L'utilisateur peut ensuite saisir le mot de passe approprié au niveau Windows et réutiliser l'ordinateur.

L'utilisateur a oublié le mot de passe

Dans ce cas, une réinitialisation du mot de passe est requise.

1. La procédure Challenge/Réponse permettra à l'utilisateur de se connecter à partir de l'authentification au démarrage.
2. Le mot de passe Windows doit être changé. Cela requiert d'autres actions de récupération hors de portée de la procédure challenge/réponse. Deux méthodes permettent de réinitialiser le mot de passe Windows :
   - via un compte de service ou administrateur disponible sur l'ordinateur final avec les droits Windows requis ;
   - via un disque de réinitialisation de mot de passe Windows.

     En tant que responsable support, vous pouvez conseiller à l'utilisateur la procédure à appliquer et lui fournir les informations d'identification Windows supplémentaires ou le disque requis :
3. L'utilisateur entre le nouveau mot de passe au niveau Windows.
4. SafeGuard Enterprise détecte que le mot de passe enregistré dans SafeGuard Enterprise ne correspond plus au mot de passe Windows. L'utilisateur est invité à saisir l'ancien mot de passe, puis doit cliquer sur **Annuler**.
5. Lorsque le mot de passe SafeGuard Enterprise est réinitialisé, un nouveau certificat doit être généré. L'utilisateur doit donc confirmer cette procédure une nouvelle fois.
6. Un nouveau certificat utilisateur est créé. Cela permet à l'utilisateur de se reconnecter à l'ordinateur ainsi qu'à l'authentification au démarrage à l'aide du nouveau mot de passe.

Remarque: Clés pour SafeGuard Data Exchange

Lorsque l'utilisateur a oublié le mot de passe Windows et doit en saisir un nouveau, un nouveau certificat utilisateur est également créé. L'utilisateur ne pourra donc plus utiliser les clés déjà créées pour SafeGuard Data Exchange. Pour continuer à utiliser les clés utilisateur déjà générées pour SafeGuard Data Exchange, l'utilisateur doit se souvenir des passphrases SafeGuard Data Exchange afin de les réactiver.

23.10.2 Génération d'une réponse pour les ordinateurs non gérés à l'aide du fichier de récupération de clé

Remarque: Le fichier de récupération de clé généré durant l'installation du logiciel de chiffrement SafeGuard Enterprise doit être stocké dans un emplacement accessible au responsable support et son nom doit être connu.

Pour générer une réponse, procédez comme suit :

1. Pour ouvrir l'assistant de récupération dans SafeGuard Management Center, sélectionnez **Outils > Récupération** dans la barre de menus.
2. Dans **Type de récupération**, sélectionnez **Clients Sophos SafeGuard (autonomes)**.
3. Cliquez sur **Parcourir** pour localiser le fichier de récupération de clé requis. Pour faciliter l'identification des fichiers de récupération, leur nom est identique à celui de l'ordinateur : nomordinateur.GUID.xml.
4. Saisissez le code de challenge que l'utilisateur vous a indiqué, puis cliquez sur **Suivant**. Ce code est vérifié.

Si le code de challenge a été saisi correctement, l'action de récupération demandée par l'ordinateur, ainsi que les actions de récupération possibles s'affichent. S'il a été saisi de façon incorrecte, le terme **Non valide** s'affiche au-dessous du bloc contenant l'erreur.

5. Sélectionnez l'action que l'utilisateur doit entreprendre, puis cliquez sur **Suivant**.
6. Un code de réponse est généré. Communiquez-le à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

L'utilisateur peut saisir le code de réponse, exécuter l'action requise, puis reprendre son travail.

24 Récupération du système

SafeGuard Enterprise chiffre les fichiers et les lecteurs de façon transparente. Les lecteurs d'initialisation peuvent également être chiffrés et les fonctions de déchiffrement telles que le code, les algorithmes de chiffrement et la clé de chiffrement doivent être disponibles très tôt au cours la phase d'initialisation. C'est la raison pour laquelle les informations chiffrées ne sont pas accessibles si les modules essentiels de SafeGuard Enterprise ne sont pas disponibles ou ne fonctionnent pas.

Les sections suivantes couvrent les sources d'erreur et les méthodes de récupération envisageables.

24.1 Récupération de données via l'initialisation à partir d'un support externe

Ce type de récupération s'applique lorsque l'utilisateur peut toujours se connecter à partir de l'authentification au démarrage mais ne peut plus accéder au volume chiffré. Dans ce cas, vous pouvez récupérer l'accès aux données chiffrées en initialisant l'ordinateur via un disque de récupération Windows PE personnalisé pour SafeGuard Enterprise.

Conditions préalables :

- L'utilisateur exécutant l'initialisation à partir d'un support externe doit disposer de l'autorisation appropriée. Ce droit peut être soit configuré dans SafeGuard Management Center via une stratégie de type Authentification (l'utilisateur peut déchiffrer le volume défini sur Oui), soit obtenu, pour une utilisation unique, via une procédure Challenge/Réponse.
- L'ordinateur doit prendre en charge l'initialisation à partir de supports autres qu'un disque dur fixe.

Pour récupérer l'accès aux données chiffrées sur l'ordinateur, procédez comme suit :

1. Demandez au support technique de vous fournir le disque Windows PE SafeGuard Enterprise.

   Le support peut télécharger le disque de récupération Windows PE avec les derniers pilotes du filtre Sophos SafeGuard sur le site du support Sophos. Pour en savoir plus, consultez la base de connaissances : http://www.sophos.com/support/knowledgebase/article/108805.html.

2. Connectez-vous à l'authentification au démarrage avec vos informations d'identification.
3. Insérez le disque de récupération Windows PE dans l'ordinateur.

4. Dans la boîte de dialogue de connexion de l'authentification au démarrage, sous **Poursuivre l'initialisation à partir de :** , sélectionnez **support externe**. L'ordinateur démarre.

L'accès aux données stockées sur cette partition est récupéré.

24.2 MBR (Master Boot Record) corrompu

Pour résoudre les problèmes de MBR corrompu, SafeGuard Enterprise propose l'utilitaire BE_Restore.exe.

Pour une description détaillée de la façon de restaurer un MBR corrompu au moyen de cet utilitaire, reportez-vous au guide des outils SafeGuard.

24.3 Code

Un disque dur dont le code d'initialisation du noyau est endommagé reste accessible car les clés sont stockées séparément du noyau dans la zone de stockage des clés (KSA). En séparant le noyau et les clés, ce type de lecteur peut être déchiffré lorsqu'il est connecté à un autre ordinateur.

Pour ce faire, l'utilisateur qui se connecte à l'autre ordinateur a besoin d'une clé de la KSA pour la partition qui ne peut être initialisée dans son jeu de clés.

Dans le pire des cas, la partition est seulement chiffrée avec le Boot_Key de l'autre ordinateur. Dans une telle situation, le responsable principal de la sécurité ou le responsable récupération doit attribuer ce Boot_Key à l'utilisateur.

Pour obtenir une description détaillée de cette procédure, reportez-vous à voir *« Asservissement » d'un disque dur* , page 266.

24.4 Volumes

SafeGuard Enterprise permet le chiffrement basé sur lecteur. Cela inclut les informations de chiffrement de l'enregistrement constituées du secteur d'initialisation, de la KSA principale et de sauvegarde, ainsi que du secteur d'initialisation original sur chaque lecteur.

Dès que l'une des unités ci-dessous est endommagée, le volume ne peut plus accéder :

- à l'une des deux zones de stockage des clés (KSA) ;
- au MBR original.

24.4.1 Secteur d'initialisation

Au cours du processus de chiffrement, le secteur d'initialisation d'un volume est remplacé par le secteur d'initialisation de SafeGuard Enterprise.

Le secteur d'initialisation de SafeGuard Enterprise contient des informations sur :

- l'emplacement de la KSA principale et de sauvegarde dans les clusters et les secteurs en relation au début de la partition ;
- la taille de la KSA.

Même si le secteur d'initialisation de SafeGuard Enterprise est endommagé, les volumes chiffrés restent inaccessibles.

L'utilitaire BE_Restore peut restaurer le secteur d'initialisation endommagé. Pour une description détaillée de cet utilitaire, reportez-vous au guide des outils SafeGuard.

24.4.2 Secteur d'initialisation original

Le secteur d'initialisation original est celui qui est exécuté après le déchiffrement du DEK (clé de chiffrement de données) et après que l'algorithme et la clé ont été chargés dans le pilote du filtre BE.

Si ce secteur d'initialisation est défectueux, Windows n'a pas accès au volume. Normalement le message d'erreur habituel « Le disque n'est pas formaté. Voulez-vous le formater maintenant ? Oui/Non » est affiché.

Néanmoins, SafeGuard Enterprise charge le DEK pour ce volume. L'outil utilisé pour réparer le secteur d'initialisation doit être compatible avec le filtre de volume supérieur de SafeGuard Enterprise.

24.5 Problèmes d'initialisation Windows

Sa conception cryptographique de la clé spécifique du volume (secteur d'initialisation, zone de stockage des clés KSA) confère à SafeGuard Enterprise une très grande souplesse.

Vous pouvez enregistrer un système endommagé en initialisant un support de restauration à partir de la fonction d'authentification au démarrage de SafeGuard Enterprise (Windows PE avec le sous-système de chiffrement de SafeGuard Enterprise installé). Ces supports ont un accès de chiffrement/déchiffrement transparent aux volumes chiffrés avec SafeGuard Enterprise. Il est possible de remédier ici à la cause du système qui ne peut être initialisé.

24.5.1 Sous-système de chiffrement

BEFLT.sys est par exemple un système de chiffrement. Effectuez la procédure décrite dans Problèmes d'initialisation Windows et réparez le système.

24.5.2 Problèmes GINA

Les problèmes GINA, par exemple les boucles circulaires, peuvent être résolus de la manière suivante : effectuez la procédure décrite dans Problèmes d'initialisation Windows et réparez le système.

24.6 Configuration de WinPE pour SafeGuard Enterprise

Pour accéder aux lecteurs chiffrés avec le BOOTKEY d'un ordinateur dans un environnement WinPE, SafeGuard Enterprise propose Win PE avec les modules de fonction et les pilotes SafeGuard Enterprise appropriés. Pour lancer SetupWinPE 2.0, entrez la commande suivante :

SetupWinPE -pe2 <fichier d'image WinPE>

fichier d'image WinPE étant le nom de chemin complet d'un fichier d'image WinPE 2.0

SetupWinPE effectue toutes les modifications nécessaires.

Remarque: Notez que, dans ce type d'environnement WinPE, seuls les lecteurs chiffrés avec le BOOTKEY sont accessibles. Les lecteurs chiffrés avec une clé utilisateur sont inaccessibles car les clés ne sont pas disponibles dans cet environnement.

24.7 « Asservissement » d'un disque dur

SafeGuard Enterprise permet l'asservissement des volumes ou des disques durs chiffrés. Il permet à l'utilisateur final, à l'administrateur Windows et au responsable de la sécurité de SafeGuard Enterprise de se connecter ou de supprimer de nouveaux volumes ou disques durs en dépit du chiffrement basé sur secteur.

La zone de stockage des clés (KSA) d'un volume contient toutes les informations nécessaires, c'est-à-dire :

- la clé générée de manière aléatoire (DEK) ;
- un ID de l'algorithme de chiffrement utilisé pour chiffrer le volume ;
- la liste des GUID utilisés pour les KEK, pouvant chiffrer et déchiffrer le DEK ;
- le volume lui-même contient sa taille.

Un volume chiffré avec SafeGuard Enterprise est accessible à partir de tous les ordinateurs protégés par SafeGuard Enterprise, à condition que l'utilisateur ou l'ordinateur possède un KEK de la KSA du volume dans son jeu de clés.

Les utilisateurs ou les ordinateurs doivent pouvoir déchiffrer le DEK chiffré par le KEK.

Un grand nombre d'utilisateurs et d'ordinateurs peuvent accéder à un volume ayant été chiffré avec un KEK distribuable tel qu'un OU, un groupe, ou une clé de domaine, car de nombreux utilisateurs/ordinateurs d'un domaine ont cette clé dans leurs jeux de clés.

Toutefois, un volume qui n'est chiffré qu'avec la clé d'initialisation individuelle (« Boot_nomdelamachine ») de l'ordinateur protégé par SafeGuard Enterprise n'est accessible que depuis cet ordinateur particulier.

Si un volume ne s'initialise pas sur son ordinateur d'origine, il peut être « asservi » sur un autre ordinateur protégé par SafeGuard Enterprise. Toutefois, la clé d'initialisation correcte n'est pas accessible. Elle doit être rendue accessible.

Chaque fois que l'utilisateur tente d'accéder au volume depuis un autre ordinateur, il peut le faire car les KEK de la KSA et le jeu de clés des autres utilisateurs ou ordinateurs correspondent de nouveau.

24.7.1 Exemple

Alice possède sa clé utilisateur personnelle. Chaque fois qu'elle est connectée à son autre ordinateur (« Laptop_Alice »), elle ne peut pas accéder au volume chiffré avec la clé d'initialisation de l'ordinateur « SGNCLT ».

Le « SGMCLT » de l'ordinateur protégé par SafeGuard Enterprise n'a que sa propre clé d'initialisation, BOOT_SGMCLT.

Le responsable de la sécurité attribue la clé d'initialisation « BOOT_SGMCLT » à Alice de la façon suivante :

1. Il sélectionne l'utilisateur Alice.
2. Il clique sur l'icône « Jumelles » dans la barre d'outils de SafeGuard Enterprise. Cela ouvre la boîte de dialogue de recherche qui affiche également les clés d'initialisation.
3. Il sélectionne la clé « BOOT_SGMCLT ».

Alice possède désormais deux clés: « User_Alice » et « BOOT_SGMCLT ». Ceci peut être vérifié dans **Clés et certificats**.

La clé « BOOT_SGMCLT » a été attribuée deux fois: à l'ordinateur SGMCLT et à l'utilisateur Alice.

Alice peut désormais accéder au volume chiffré de n'importe quel autre ordinateur final protégé par SafeGuard Enterprise auquel elle peut se connecter.

Ensuite, elle peut facilement utiliser des outils tels que l'Explorateur Windows ou regedit.exe pour résoudre la cause du problème d'initialisation.

Si, dans le cas le moins favorable, le problème ne peut pas être résolu, elle peut enregistrer les données sur une autre unité, reformater le volume et le reconfigurer entièrement.

25 Données d'inventaire et d'état

SafeGuard Enterprise lit une quantité considérable de données d'inventaire et d'état provenant des ordinateurs finaux. Ces données indiquent l'état général connu de chaque ordinateur. Ces données s'affichent clairement dans SafeGuard Management Center, dans la zone **Utilisateurs & ordinateurs** dans l'onglet **Inventaire**.

En tant que responsable de la sécurité, vous pouvez afficher et imprimer les données d'inventaire et d'état affichées dans SafeGuard Management Center. Par exemple, vous pouvez imprimer des rapports pour prouver que des périphériques finals ont été chiffrés. Les fonctions de tri et de filtrage étendus vous aident à sélectionner les données pertinentes.

L'**inventaire** propose, par exemple, les données suivantes sur chaque machine :

- stratégie appliquée ;
- état de chiffrement de tous les supports ;
- état du POA et type de POA ;
- données sur les modules SafeGuard Enterprise installés ;
- état de l'éveil par appel réseau sécurisé (WOL) ;
- données utilisateur.

25.1 Affichage des données d'inventaire

Les données d'inventaire sont accessibles comme suit :

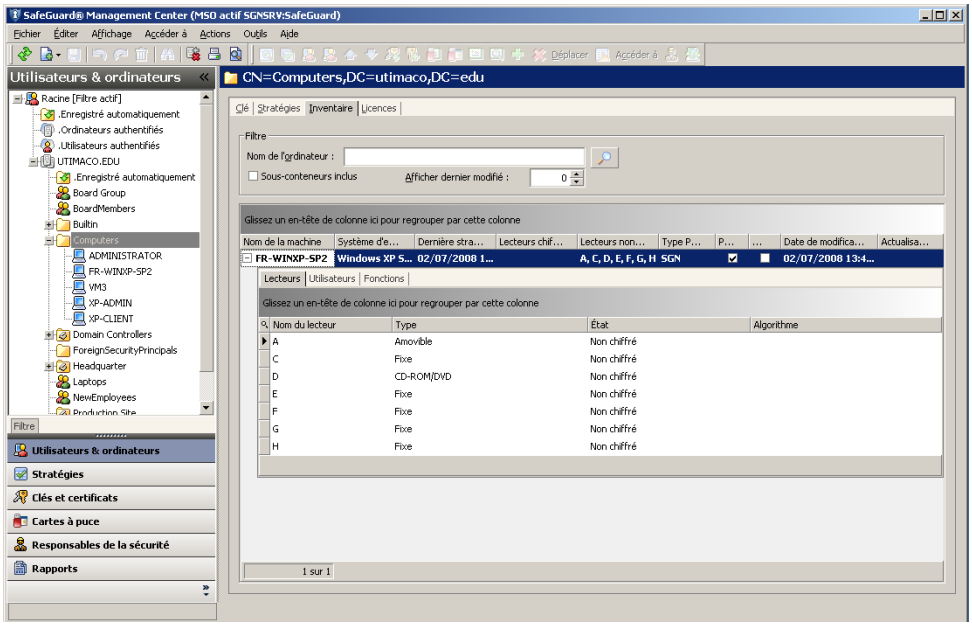
Ouvrez SafeGuard Management Center.

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur le bouton **Utilisateurs & ordinateurs**.
2. Dans la fenêtre de navigation, cliquez sur le conteneur concerné (domaine, groupe de travail ou ordinateur) à gauche.
3. Dans la zone d'action, accédez à l'onglet **Inventaire** à droite.
4. Dans la zone **Filtre**, sélectionnez le filtre à appliquer à l'écran d'inventaire, voir *Filtrage des données d'inventaire* en page 270.

Avis : si vous sélectionnez un ordinateur particulier, les données d'inventaire sont reçues dès que vous accédez à l'onglet **Inventaire**. La zone **Filtre** n'est pas disponible ici.

5. Dans la zone **Filtre**, cliquez sur la loupe.

Les données d'inventaire et d'état s'affichent sous forme de tableau récapitulatif de toutes les machines du conteneur sélectionné. Les onglets **Lecteurs**, **Utilisateurs** et **Fonctions** sont également disponibles pour chaque machine.

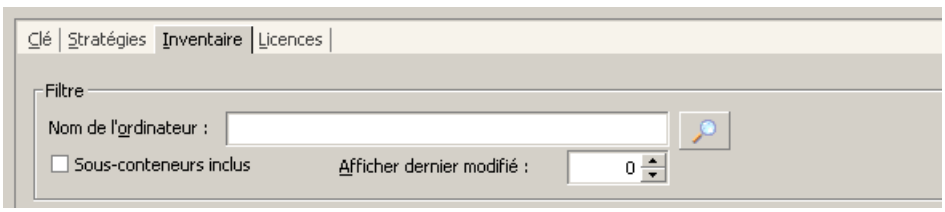


Cliquez sur l'en-tête de la colonne pour trier les données de l'inventaire par les valeurs de la colonne sélectionnée. Le menu contextuel de chaque colonne propose de nombreuses fonctions de tri, de regroupement et de réglage de l'affichage.

25.1.1 Filtrage des données d'inventaire

Lorsque vous utilisez un OU, des filtres peuvent être définis pour limiter l'affichage en fonction de critères particuliers.

Les champs suivants sont disponibles pour définir des filtres dans la zone **Filtre** de l'onglet **Inventaire** :



Champ	Description
Nom de l'ordinateur	Pour afficher les données d'inventaire et d'état d'un ordinateur particulier, entrez le nom de l'ordinateur dans ce champ.
Sous-conteneurs inclus	Activez ce champ pour inclure les sous-conteneurs à l'écran.
Afficher dernier modifié	Utilisez ce champ pour spécifier le nombre de dernières modifications à afficher.

Vous pouvez également utiliser l'éditeur de filtres pour créer des filtres définis par l'utilisateur. Vous pouvez ouvrir l'éditeur de filtres via le menu contextuel de chaque colonne. Dans la fenêtre **Générateur de filtres**, vous pouvez définir des filtres personnalisés et les appliquer à la colonne concernée.

25.1.2 Actualisation des données d'inventaire

Le PC de l'utilisateur envoie et met généralement à jour les données d'inventaire lorsqu'elles sont modifiées.

La commande **Demander une actualisation de l'inventaire** peut être utilisée pour demander manuellement une actualisation des données d'inventaire actuelles de l'ordinateur. Cette commande est disponible pour un ordinateur particulier ou pour tous les ordinateurs d'un nœud (pouvant inclure des nœuds secondaires) via le menu contextuel et le menu **Actions** de la barre de menus SafeGuard Management Center. La commande peut également être sélectionnée via le menu contextuel des entrées de la liste.

Si vous sélectionnez cette commande ou que vous cliquez sur l'icône **Demander une actualisation de l'inventaire** dans la barre d'outils, les ordinateurs concernés envoient leurs données d'inventaire actuelles.

C'est également le cas avec d'autres zones de Management Center : pour actualiser l'écran dans SafeGuard Management Center, vous pouvez utiliser la commande **Actualiser** accessible dans le menu contextuel des ordinateurs individuels ou de tous les ordinateurs d'un nœud et dans le menu **Affichage** de la barre de menus. Vous pouvez également utiliser l'icône à double flèche d'**actualisation** dans la barre d'outils pour actualiser l'affichage.

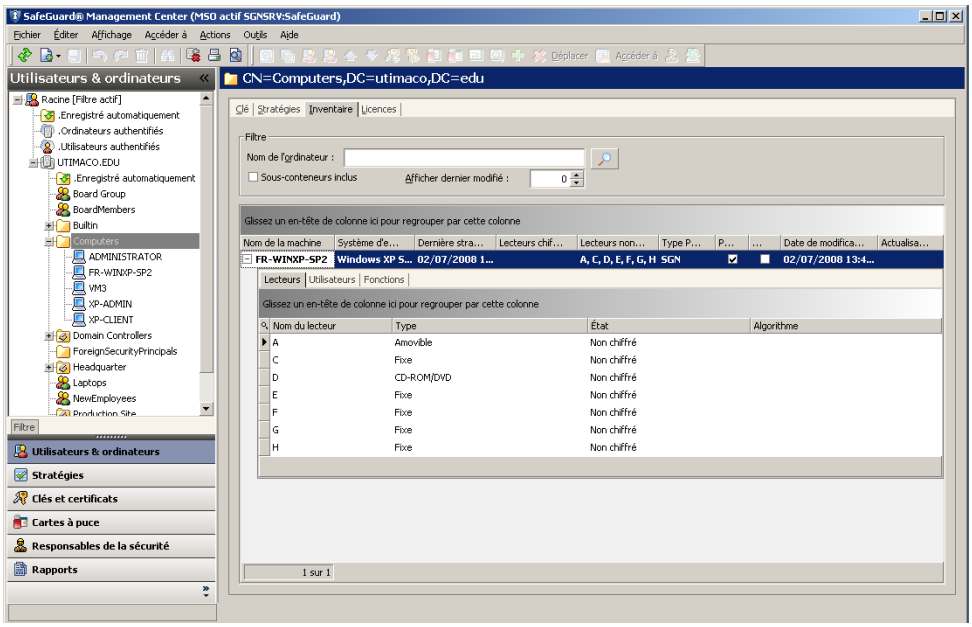
25.1.3 Présentation

Les colonnes individuelles dans la présentation proposant les informations suivantes :

Colonne	Explication
Nom de la machine	Indique le nom de l'ordinateur.
Système d'exploitation	Indique le système d'exploitation de l'ordinateur.
Dernière stratégie reçue	Indique quand (date et heure) l'ordinateur a reçu la dernière stratégie.
Lecteurs chiffrés	Indique les lecteurs chiffrés de l'ordinateur.
Lecteurs non chiffrés	Indique les lecteurs non chiffrés de l'ordinateur.
Type POA	Spécifie si l'ordinateur concerné est un client BitLocker ou un client SafeGuard Enterprise natif.
POA	Spécifie si l'authentification au démarrage est activée pour l'ordinateur.
Éveil par appel réseau	Spécifie si l'éveil par appel réseau est activé pour l'ordinateur.
Date de modification	Indique la date à laquelle les données d'inventaire ont changé en raison d'une demande d'actualisation de l'inventaire ou de l'envoi de l'ordinateur de nouvelles données d'inventaire.
Actualisation demandée	Indique la date de la dernière demande d'actualisation. La valeur affichée dans ce champ sera supprimée une fois la demande traitée par l'ordinateur.
DSN parent	Indique le nom distinctif de l'objet conteneur auquel l'ordinateur est subordonné. Cette colonne ne s'affiche que si le champ **Sous-conteneurs inclus** a été activé dans la zone **Filtre**.

25.1.4 Onglet Lecteurs

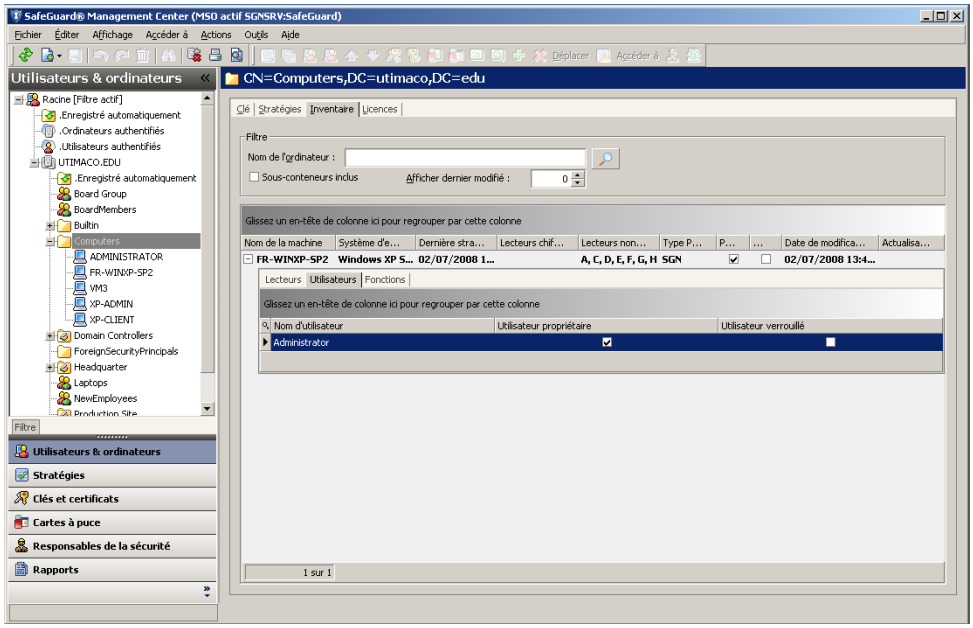
L'onglet **Lecteurs** indique les données d'inventaire et d'état des lecteurs sur l'ordinateur concerné.



Colonne	Explication
Nom du lecteur	Indique le nom du lecteur.
Type	Indique le type de lecteur (fixe, amovible ou CD-ROM/DVD par exemple).
État	Indique l'état de chiffrement du lecteur.
Algorithme	Pour les lecteurs chiffrés, ce champ indique l'algorithme utilisé pour le chiffrement.

25.1.5 Onglet Utilisateurs

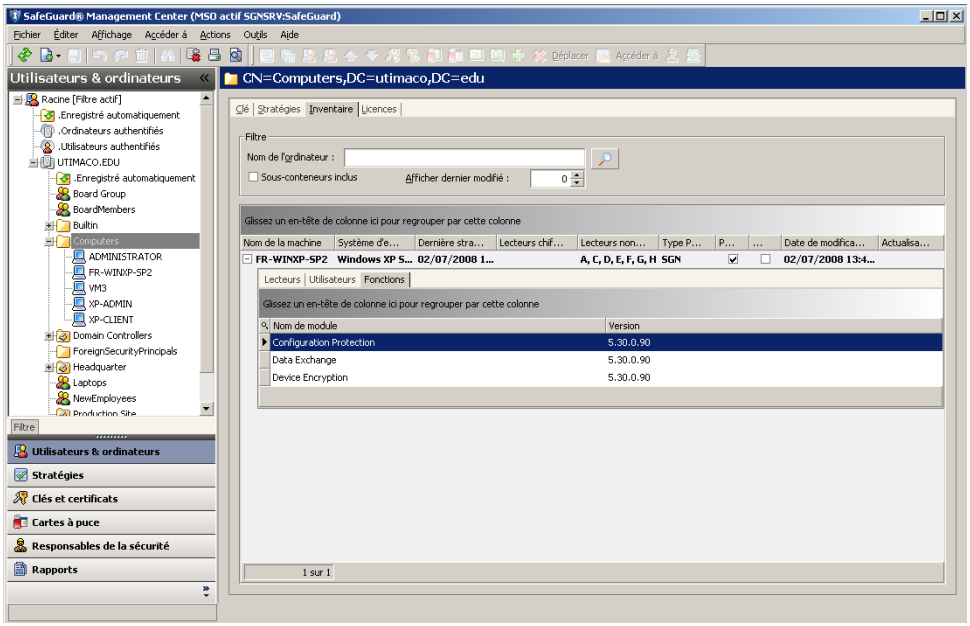
L'onglet **Utilisateurs** indique les données d'inventaire et d'état des utilisateurs sur l'ordinateur concerné.



Colonne	Explication
Nom d'utilisateur	Indique le nom d'utilisateur de l'utilisateur concerné.
Utilisateur propriétaire	Spécifie si l'utilisateur est défini comme étant le propriétaire de la machine.
Utilisateur verrouillé	Spécifie si l'utilisateur est verrouillé.

25.1.6 Onglet Fonctions

L'onglet **Fonctions** propose une présentation de tous les modules SafeGuard Enterprise installés sur l'ordinateur.



Colonne	Explication
Nom du module	Indique le nom du module SafeGuard Enterprise installé.
Version	Indique la version logicielle du module SafeGuard Enterprise installé.

25.2 Impression de rapports d'inventaire

Les données affichées dans l'onglet **Inventaire** peuvent être imprimées sous forme de rapports d'inventaire à l'aide du menu **Fichier** dans la barre de menus de SafeGuard Management Center.

Pour obtenir un aperçu avant impression, sélectionnez **Fichier** > **Aperçu avant impression**. L'aperçu avant impression propose diverses fonctions comme l'exportation du document dans une large gamme de formats de sortie (fichier .PDF par exemple) ou la modification de la mise en page (en-tête et pied de page par exemple).

Pour imprimer le document immédiatement, sélectionnez **Fichier** > **Imprimer**.

26 Rapports

La possibilité de signaler des incidents liés à la sécurité est une condition préalable à une analyse détaillée du système. Les événements consignés simplifient le suivi exact des processus sur un poste de travail donné ou sur un réseau. En consignant les événements, vous pouvez, par exemple, vérifier les failles de sécurité dues à des tiers. La fonction de consignation aide également l'administrateur ou le responsable de la sécurité à déterminer des erreurs en accordant des droits utilisateur et en les corrigeant.

SafeGuard Enterprise consigne toutes les activités de l'ordinateur final et les informations d'état, ainsi que les actions de l'administrateur et les événements liés à la sécurité, puis les enregistre de manière centralisée. La fonction de consignation enregistre les événements déclenchés par des produits SafeGuard installés. Le type des journaux est défini dans des stratégies de consignation. C'est dans celles-ci que vous spécifiez également l'emplacement de sortie et d'enregistrement des événements consignés : le journal des événements Windows de l'ordinateur final concerné ou la base de données SafeGuard Enterprise.

À condition de disposer des droits requis de responsable de la sécurité, vous pouvez afficher, imprimer et archiver les informations d'état et les rapports de journaux affichés dans SafeGuard Management Center. SafeGuard Management Center propose des fonctions de tri et de filtrage complètes très utiles lors de la sélection d'événements pertinents à partir des informations disponibles.

Des analyses automatiques de la base de données de journaux, via Crystal Reports ou Microsoft System Center Operations Manager par exemple, sont également possibles. SafeGuard Enterprise protège les entrées des journaux contre toute manipulation non autorisée à l'aide de signatures sur le client et sur le serveur.

En fonction de la stratégie de consignation définie et attribuée, les événements des catégories suivantes peuvent être consignés :

- Authentification
- Administration
- Système
- Chiffrement
- Client
- Communication
- Contrôle d'accès

26.1 Scénarios d'application

La fonction de consignation de SafeGuard Enterprise est une solution conviviale et complète d'enregistrement et d'analyse d'événements. Les exemples suivants illustrent des scénarios d'application types de la fonction **Rapports** de SafeGuard Enterprise.

Contrôle centralisé des postes de travail d'un réseau

Le responsable de la sécurité souhaite être régulièrement informé des événements critiques (accès non autorisé aux données, nombre d'échecs de tentatives de connexion sur une période spécifiée, par exemple). Grâce à une stratégie de consignation, le responsable de la sécurité peut configurer la consignation dans un fichier journal local de processus afin de consigner tous les événements liés à la sécurité survenus sur les ordinateurs finaux concernés. Ce fichier journal est transféré dans la base de données SafeGuard Enterprise via SafeGuard Enterprise Server une fois le nombre d'événements spécifié dans une autre stratégie atteint. Le responsable de la sécurité peut récupérer, afficher et analyser les événements dans la **Visionneuse des événements** de SafeGuard Management Center. Les processus exécutés sur différents ordinateurs finaux peuvent ainsi être audités sans intervention du personnel sur la consignation.

Contrôle des utilisateurs mobiles

Les utilisateurs mobiles ne sont généralement pas connectés en permanence au réseau de l'entreprise. Par exemple, les commerciaux sur le terrain déconnectent leur portable pendant une réunion. Dès qu'ils se reconnectent au réseau, les événements SafeGuard Enterprise consignés pendant la période hors ligne sont transférés. La fonction de consignation propose ainsi une vue d'ensemble précise des activités de l'utilisateur pendant la période de déconnexion de l'ordinateur correspondant.

26.2 Condition préalable

Une machine sur laquelle seul SafeGuard Enterprise Management Center est installé n'est pas connectée au serveur après l'installation initiale. Pour utiliser la fonction de consignation, le package client doit être exécuté sur la machine. La machine est alors activée en tant que client sur le serveur et la fonction de consignation peut être utilisée.

Pour plus d'informations sur les packages clients, consultez le manuel d'installation de SafeGuard Enterprise.

26.3 Destinations des événements consignés

Deux destinations des événements consignés sont possibles : la visionneuse des événements Windows ou la base de données SafeGuard Enterprise. Seuls les événements liés à un produit SafeGuard sont inscrits à la destination correspondante.
Les destinations de sortie des événements à consigner sont spécifiées dans la stratégie de consignation.

26.3.1 Visionneuse des événements Windows

Les événements, pour lesquels vous définissez la visionneuse des événements Windows comme destination dans la stratégie de consignation, sont consignés dans la visionneuse des événements Windows. La visionneuse des événements Windows peut être utilisée pour afficher et gérer les journaux des événements liés au système, à la sécurité et à l'application. Vous pouvez également enregistrer ces journaux d'événements. Un compte administrateur sur l'ordinateur final concerné est requis pour ces procédures. Dans la visionneuse des événements Windows, un code d'erreur s'affiche à la place d'un texte descriptif de l'événement.

Avis : ce chapitre décrit les processus d'affichage, de gestion et d'analyse des journaux d'événements dans SafeGuard Management Center. Pour plus d'informations sur l'affichage et la gestion des journaux d'événements via la visionneuse des événements Windows, consultez votre documentation Microsoft.

26.3.2 Base de données SafeGuard Enterprise

Les événements, pour lesquels vous définissez la base de données SafeGuard Enterprise comme destination dans la stratégie de consignation, sont collectés dans un fichier journal local dans le cache local de l'ordinateur final concerné dans le répertoire auditing\SGMTranslog. Les fichiers journaux sont soumis à un mécanisme de transport qui les transfère dans la base de données via SafeGuard Enterprise Server. Par défaut, le fichier est soumis dès que le mécanisme de transport a établi une connexion avec le serveur. Pour limiter la taille d'un fichier journal, vous pouvez définir un nombre maximal d'entrées du journal dans une stratégie du type **Paramètres généraux**. Le fichier journal est soumis dans la file d'attente de transport de SafeGuard Enterprise Server une fois le nombre d'entrées spécifié atteint. Les événements consignés dans la base de données centrale peuvent être affichés dans la **Visionneuse des événements** SafeGuard Enterprise. En tant que responsable de la sécurité, vous devez disposer des droits appropriés pour afficher, analyser et gérer les événements consignés dans la base de données.

26.4 Définition des paramètres de consignation

Les paramètres de rapport sont définis à l'aide de deux stratégies :

- Stratégie **Paramètres généraux**
  Dans une stratégie **Paramètres généraux**, vous pouvez spécifier un nombre maximum d'entrées consignées au-delà duquel le fichier journal contenant les événements destinés à la base de données centrale doit être transféré dans la base de données de SafeGuard Enterprise. Ceci permet de réduire la taille des fichiers journaux individuels à transférer. Ce paramètre est facultatif.

- Stratégie de **consignation**
  Les événements à consigner sont spécifiés dans une stratégie de consignation. Dans cette stratégie, un responsable de la sécurité disposant des droits de stratégie requis définit les événements à consigner vers une destination de sortie spécifique.

Les deux sections suivantes décrivent comment définir ces deux stratégies de consignation.

26.4.1 Définition du nombre d'événements pour commentaires

Pour définir le nombre maximum d'entrées consignées d'un fichier journal, procédez de la façon suivante :

Vous vous trouvez dans la zone **Stratégies** de Management Center.

1. Créez une stratégie **Paramètres généraux** ou sélectionnez une stratégie existante.
2. Dans le champ **Commentaires après un certain nombre d'événements**, spécifiez le nombre maximum d'événements d'un fichier journal.
3. Enregistrez vos paramètres.

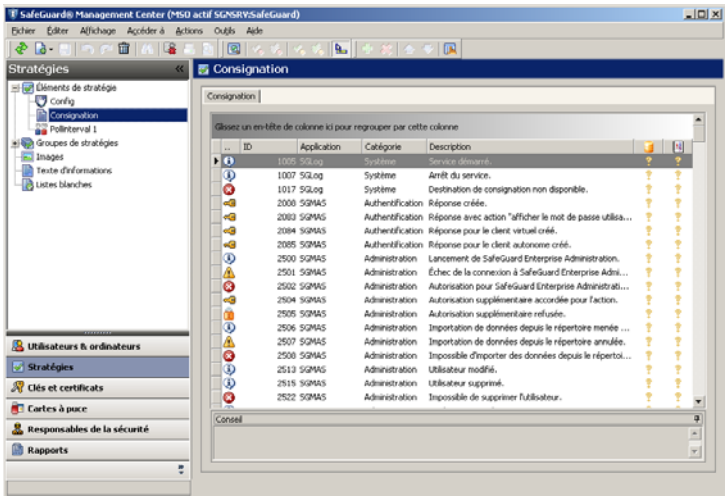
Le nombre d'événements spécifié s'applique à la consignation une fois la stratégie attribuée.

26.4.2 Sélection d'événements

Pour sélectionner les événements à consigner, procédez de la façon suivante :

Vous vous trouvez dans la zone **Stratégies** de Management Center.

1. Créez une stratégie **Consignation** ou sélectionnez une stratégie existante.
2. Dans la zone d'action de droite, tous les événements prédéfinis comme pouvant être consignés s'affichent sous **Consignation**. Cliquez sur les en-têtes de colonnes pour trier les événements par **ID**, **Catégorie**, etc.



3. Pour spécifier qu'un événement doit être consigné dans la base de données SafeGuard Enterprise, sélectionnez l'événement en cliquant sur la colonne contenant l'icône de base de données **Consigner les événements dans une base de données**. Pour les événements à consigner dans la visionneuse des événements Windows, cliquez sur la colonne contenant l'icône de journal d'événements **Consigner dans le journal des événements**. Cliquez plusieurs fois pour désélectionner l'événement ou le rendre nul. Si vous ne définissez pas de paramètre pour un événement, la valeur par défaut correspondante s'applique. Pour afficher les valeurs par défaut valides, cliquez sur l'icône de valeur par défaut **Afficher les valeurs par défaut des paramètres non configurés** dans la barre d'outils de SafeGuard Management Center.

Avis : vous pouvez également spécifier ces paramètres via le menu contextuel des événements individuels.

4. Pour tous les événements sélectionnés pour la consignation, une coche verte s'affiche dans la colonne correspondante.
   Enregistrez vos paramètres.

Les événements sélectionnés sont consignés dans la destination de sortie correspondante une fois la stratégie attribuée.

Événements disponibles

Pour obtenir une liste de tous les événements pouvant être consignés, voir *Événements disponibles pour les rapports* en page 298.

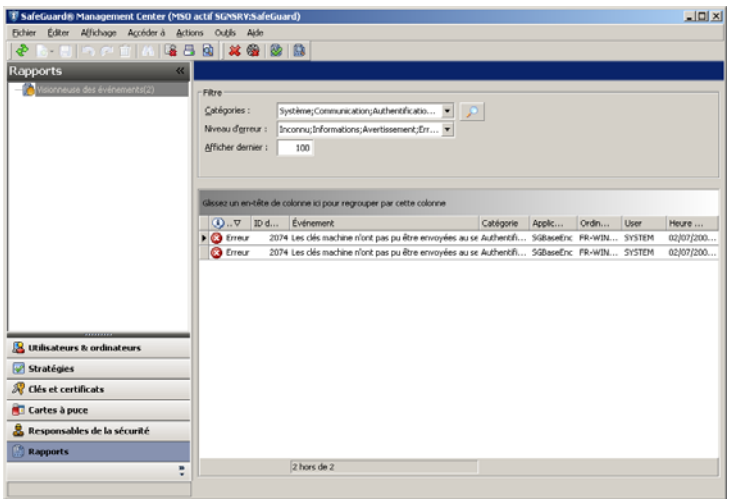
26.5 Affichage des événements consignés

Si vous disposez des droits requis de responsable de la sécurité, vous pouvez afficher les événements consignés dans la base de données centrale dans la visionneuse des événements SafeGuard Management Center.

Pour récupérer les entrées consignées dans la base de données centrale, procédez de la façon suivante :

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Rapports**.
2. Dans la zone d'action **Visionneuse des événements** de droite, cliquez sur la loupe.

Tous les événements consignés dans la base de données centrale sont affichés dans la visionneuse des événements.



Les colonnes indiquent les informations suivantes relatives aux événements consignés :

Colonne	Description
Niveau (icône)	Affiche une icône indiquant la classification de l'événement (avertissement, erreur, par exemple).
ID d'événement	Affiche un numéro identifiant l'événement.
Événement	Affiche un texte d'événement (une description de l'événement).
Catégorie	Classification de l'événement selon la source (Chiffrement, Authentification, Système, par exemple).
Application	Affiche la zone logicielle d'où l'événement provient (SGMAuth, SGBaseENc, SGMAS, par exemple).
Ordinateur	Affiche le nom de l'ordinateur sur lequel l'événement consigné s'est produit.
Domaine de l'ordinateur	Affiche le domaine de l'ordinateur sur lequel l'événement consigné s'est produit.
Utilisateur	Affiche l'utilisateur connecté lorsque l'événement s'est produit.
Domaine utilisateur	Affiche le domaine de l'utilisateur connecté lorsque l'événement s'est produit.
Heure de connexion	Affiche la date et l'heure système auxquelles l'événement a été consigné sur l'ordinateur final.

Cliquez sur les en-têtes de colonnes pour trier les événements par **Niveau**, **Catégorie**, etc.

Le menu contextuel des colonnes propose également de nombreuses fonctions de tri, de regroupement et de personnalisation de la visionneuse des événements.

Double-cliquez sur une entrée de la visionneuse des événements pour afficher des détails sur l'événement consigné.

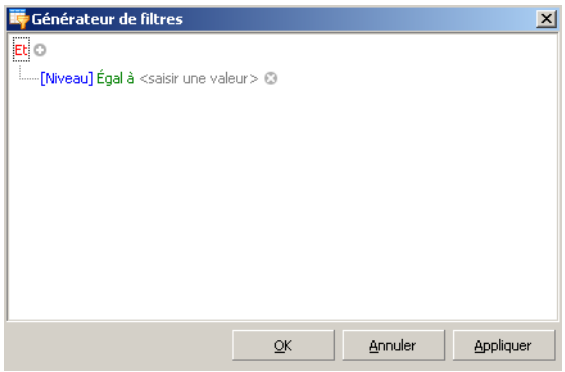
26.5.1 Application de filtres à la visionneuse des événements SafeGuard Enterprise

SafeGuard Management Center propose des fonctions de filtrage complètes. Grâce à ces fonctions, vous pouvez récupérer rapidement les événements appropriés parmi ceux affichés.

La zone **Filtre** de la **Visionneuse des événements** propose les champs suivants pour définir des filtres :

Champ	Description
Catégories	Grâce à ce champ, vous pouvez filtrer la visionneuse des événements en fonction de la classification source (par exemple, Chiffrement, Authentification, Système) indiquée dans la colonne **Catégorie**. Sélectionnez les catégories souhaitées dans la liste déroulante du champ.
Niveau d'erreur	Grâce à ce champ, vous pouvez filtrer la visionneuse des événements en fonction de la classification des événements Windows (par exemple, avertissement, erreur) indiquée dans la colonne **Niveau**. Sélectionnez les niveaux souhaités dans la liste déroulante du champ.
Afficher dernier	Dans ce champ, vous pouvez définir le nombre d'événements à afficher. Les derniers événements consignés sont affichés (par défaut, les 100 derniers événements).

Vous pouvez également créer des filtres personnalisés à l'aide de l'éditeur de filtres. Vous pouvez afficher l'éditeur de filtres via le menu contextuel des colonnes d'un rapport. Dans la fenêtre **Générateur de filtres**, vous pouvez définir des filtres et les appliquer à la colonne concernée.



26.6 Impression de rapports

Vous pouvez imprimer les rapports d'événements affichés dans la visionneuse des événements SafeGuard Management Center via le menu **Fichier** de la barre de menus de SafeGuard Management Center.

Pour afficher un aperçu avant l'impression du rapport, sélectionnez **Fichier** > **Aperçu avant impression**. L'aperçu avant impression propose différentes fonctions comme l'exportation du document dans divers formats de sortie (PDF par exemple) ou la modification de la mise en page (en-tête et pied de page par exemple).

Pour imprimer le document sans afficher l'aperçu, sélectionnez **Fichier** > **Imprimer**.

26.7 Concaténation des événements consignés

Les événements destinés à la base de données centrale sont consignés dans le tableau EVENT de la base de données de SafeGuard Enterprise. Une protection d'intégrité spécifique peut être appliquée à ce tableau et les événements peuvent être consignés sous forme de liste concaténée dans le tableau EVENT. En raison de la concaténation, chaque entrée de la liste dépend de l'entrée précédente. Si une entrée est supprimée de la liste, ceci apparaît clairement et peut être vérifié à l'aide d'une vérification de l'intégrité.

Pour optimiser les performances, la concaténation des événements dans le tableau EVENT est désactivée par défaut. Vous pouvez cependant activer la concaténation des événements consignés afin d'en vérifier l'intégrité (voir *Vérification de l'intégrité des événements consignés* en page 285).

Avis : la protection d'intégrité spécifique ne s'applique pas au tableau EVENT lorsque la concaténation des événements consignés est désactivée.

26.7.1 Activation de la concaténation des événements consignés

Pour activer la concaténation des événements, procédez comme suit :

1. Arrêtez le service Web SGNSRV sur le serveur Web.
2. Supprimez tous les événements de la base de données et créez une sauvegarde lors de la suppression (voir *Suppression de tous les événements ou des événements sélectionnés* en page 285).

Avis : si vous ne supprimez pas tous les événements antérieurs de la base de données, la concaténation n'est pas exécutée correctement puisque la concaténation n'est pas activée pour les événements antérieurs restants.

3. Définissez la clé de registre suivante sur 0 ou supprimez-la :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Utimaco\SafeGuard Enterprise
   DWORD: DisableLogEventChaining = 0
   ```

4. Redémarrez le service Web.

La concaténation des événements consignés est activée.

Pour désactiver de nouveau la concaténation des événements, définissez la clé de registre sur `1`.

26.8 Vérification de l'intégrité des événements consignés

Condition préalable : Pour vérifier l'intégrité des événements consignés, la concaténation des événements dans le tableau EVENT doit être activée.

Pour vérifier l'intégrité des événements affichés dans la **Visionneuse des événements** SafeGuard Enterprise, procédez de la façon suivante :

Vous vous trouvez dans la zone **Rapports** de Management Center.

Dans la barre de menus de SafeGuard Management Center, sélectionnez **Actions** > **Vérifier l'intégrité**. Vous pouvez également cliquer sur l'icône **Vérifier l'intégrité des événements du journal** de la barre d'outils.

Un message vous informant sur l'intégrité des événements consignés s'affiche.

Avis : si la concaténation des événements est désactivée, une erreur est renvoyée lors de la vérification des événements consignés dans SafeGuard Management Center.

26.9 Suppression de tous les événements ou des événements sélectionnés

Pour supprimer des événements sélectionnés du journal d'événements, procédez de la façon suivante :

Vous vous trouvez dans la zone **Rapports** de Management Center.

1. Dans la **Visionneuse des événements**, sélectionnez les événements à supprimer.

2. Pour supprimer les événements sélectionnés, choisissez **Actions** > **Supprimer les événements** ou cliquez sur l'**icône Supprimer les événements** de la barre d'outils.
   Pour supprimer tous les événements, sélectionnez **Actions** > **Supprimer tous les événements** ou cliquez sur l'**icône Supprimer tous les événements** de la barre d'outils.

3. Avant de supprimer les événements sélectionnés, le système affiche la fenêtre **Sauvegarder les événements sous** permettant de créer un fichier de sauvegarde (voir *Création d'un fichier de sauvegarde* en page 286).

Les événements sélectionnés sont supprimés du journal des événements.

26.10 Création d'un fichier de sauvegarde

Lors de la suppression d'événements, vous pouvez créer un fichier de sauvegarde du rapport affiché dans la visionneuse des événements SafeGuard Management Center.

Lors de la sélection de **Actions** > **Supprimer les événements** ou de **Actions** > **Supprimer tous les événements**, la fenêtre **Sauvegarder les événements sous** permettant de créer un fichier de sauvegarde s'affiche avant la suppression des événements. Pour créer un fichier de sauvegarde .XML du journal des événements, entrez un nom et un emplacement de fichier, puis cliquez sur **OK**.

26.11 Ouverture d'un fichier de sauvegarde

Pour ouvrir le fichier de sauvegarde .XML créé lors du processus de suppression, procédez de la façon suivante :

Vous vous trouvez dans la zone **Rapports** de Management Center.

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Actions** > **Ouvrir le fichier de sauvegarde**. Vous pouvez également cliquer sur l'icône **Ouvrir le fichier de sauvegarde** de la barre d'outils.

2. La fenêtre **Ouvrir une sauvegarde d'événement** s'affiche. Sélectionnez le fichier de sauvegarde à ouvrir et cliquez sur **Ouvrir**.

Le fichier de sauvegarde est ouvert et les événements s'affichent dans la visionneuse des événements SafeGuard Management Center. Pour revenir à la vue classique de la visionneuse des événements, cliquez de nouveau sur l'icône **Ouvrir le fichier de sauvegarde** de la barre d'outils.

26.12 Nettoyage d'événement planifié à l'aide d'un script

Quatre scripts SQL sont disponibles dans le répertoire \tools du CD du produit SafeGuard Enterprise pour le nettoyage automatique et fiable du tableau EVENT :

- `spShrinkEventTable_install.sql`
- `ScheduledShrinkEventTable_install.sql`
- `spShrinkEventTable_uninstall.sql`
- `ScheduledShrinkEventTable_uninstall.sql`

Les deux scripts `spShrinkEventTable_install.sql` et `ScheduledShrinkEventTable_install.sql` permettent d'installer une procédure enregistrée sur le serveur de base de données et une tâche planifiée qui exécute la procédure enregistrée à intervalle régulier et défini. La procédure enregistrée déplace des événements du tableau EVENT dans le tableau de sauvegarde EVENT_BACKUP tout en conservant un nombre prédéfini d'événements récents dans le tableau EVENT.

Les deux scripts `spShrinkEventTable_uninstall.sql` et `ScheduledShrinkEventTable_uninstall.sql` permettent de désinstaller la procédure enregistrée ainsi que la tâche planifiée et de supprimer le tableau EVENT_BACKUP.

Avis : si vous utilisez la procédure enregistrée pour déplacer des événements du tableau EVENT dans le tableau de sauvegarde, la concaténation des événements ne s'applique plus. L'activation de la concaténation tout en utilisant la procédure enregistrée pour le nettoyage des événements est donc inutile. Pour plus d'informations sur la concaténation, voir *Concaténation des événements consignés* en page 284.

26.12.1 Création de la procédure enregistrée

Le script `spShrinkEventTable_install.sql` permet de créer une procédure enregistrée qui déplace des données du tableau EVENT dans un tableau de sauvegarde EVENT_BACKUP. Le tableau EVENT_BACKUP est créé automatiquement s'il n'existe pas.

La première ligne est « USE SafeGuard ». Si vous avez donné un autre nom à votre base de données SafeGuard Enterprise, modifiez le nom en conséquence.

La procédure enregistrée conserve les <n> derniers événements dans le tableau EVENT et déplace les autres événements dans le tableau EVENT_BACKUP. Le nombre d'événements conservés dans le tableau EVENT est défini à l'aide d'un paramètre.

Pour exécuter la procédure enregistrée, lancez la commande suivante dans SQL Server Management Studio (New Query) :

```
exec spShrinkEventTable 1000
```

L'exemple de commande ci-dessus déplace tous les événements sauf les 1000 derniers.

26.12.2 Création d'une tâche planifiée d'exécution de la procédure enregistrée

Pour nettoyer automatiquement le tableau EVENT à intervalle régulier, vous pouvez créer une tâche dans SQL Server. La tâche peut être créée à l'aide du script `ScheduledShrinkEventTable_install.sql` ou via SQL Enterprise Manager.

Avis : la tâche planifiée ne s'applique pas aux bases de données SQL Express. L'agent SQL Server doit être en cours d'exécution pour que la tâche planifiée soit exécutée. SQL Server Express ne comportant aucun agent SQL Server, cette tâche ne s'applique pas à ces installations.

- Le script doit être exécuté dans msdb. Si vous avez donné un autre nom que SafeGuard à votre base de données SafeGuard Enterprise, modifiez le nom en conséquence.

  ```
  /* Default: Database name 'SafeGuard' change if required*/
  SELECT @SafeGuardDataBase='SafeGuard'
  ```

- Vous pouvez également préciser le nombre d'événements à conserver dans le tableau EVENT. Le nombre par défaut est 100 000.

  ```
  /* Default: keep the latest 100000 events, change if required*/
  SELECT @ShrinkCommand='exec spShrinkEventTable 100000'
  ```

- Vous pouvez spécifier si l'exécution de la tâche doit être consignée dans le journal d'événements NT.

  ```
  exec sp_add_job
  @job_name='AutoShrinkEventTable',
  @enabled=1,
  @notify_level_eventlog=3
  ```

  Le paramètre `notify_level_eventlog` peut prendre les valeurs suivantes :

Valeur	Résultat
3	Consignation à chaque exécution de la tâche.
2	Consignation en cas d'échec de la tâche.
1	Consignation si la tâche est exécutée avec succès.
0	Pas de consignation de l'exécution de la tâche dans le journal d'événements NT.

- Vous pouvez préciser la fréquence de répétition de la tâche en cas d'échec.
  `exec sp_add_jobstep`
  - `@retry_attempts=3`
    Cet exemple définit 3 tentatives d'exécution de la tâche en cas d'échec.
  - `@retry_interval=60`
    Cet exemple définit un intervalle de 60 minutes.
- Vous pouvez spécifier l'heure d'exécution de la tâche.
  `exec sp_add_jobschedule`
  - `@freq_type=4`
    Cet exemple définit une exécution quotidienne de la tâche.
  - `@freq_interval=1`
    Cet exemple définit une exécution de la tâche une fois par jour.
  - `@active_start_time=010000`
    Cet exemple définit que la tâche est exécutée à 1 heure du matin.

Avis : la syntaxe du paramètre `@active_start_time` indiquée ci-dessus fonctionne sous SQL Server 2005. La syntaxe correcte pour SQL Server 2000 est : `@active_start_time='1:00:00'`.

Avis : outre les valeurs d'exemple indiquées ci-dessus, vous pouvez définir différentes options de planification avec `sp_add-jobschedule`. Par exemple, la tâche peut être exécutée toutes les deux minutes ou une fois par semaine seulement. Pour plus d'informations, consultez la documentation de Microsoft Transact SQL.

26.12.3 Nettoyage des procédures enregistrées, des tâches et des tableaux

Le script `spShrinkEventTable_uninstall.sql` permet de supprimer la procédure enregistrée et le tableau EVENT_BACKUP. Le script `ScheduledShrinkEventTable_uninstall.sql` permet d'annuler l'enregistrement de la tâche planifiée.

Avis : lorsque le script `spShrinkEventTable_uninstall.sql` est exécuté, le tableau EVENT_BACKUP est supprimé ainsi que toutes les données qu'il contient.

26.13 Modèles de messages de rapport

Les événements ne sont pas consignés avec leurs textes d'événements complets dans la base de données SafeGuard Enterprise. Seuls l'ID et les valeurs de paramètre correspondantes sont inscrits dans la table de la base de données. Lors de la récupération des événements consignés dans la visionneuse des événements SafeGuard Management Center, les valeurs de paramètre et les modèles de texte contenus dans le fichier .dll sont convertis en texte d'événement complet dans la langue du système SafeGuard Management Center actuelle.

Les modèles utilisés pour le texte d'événement peuvent être modifiés et traités, à l'aide de requêtes SQL par exemple. Pour cela, vous pouvez générer une table contenant tous les modèles de texte des messages d'événement. Vous pouvez ensuite personnaliser les modèles en fonction de vos exigences particulières.

Pour créer une table contenant les modèles de texte des ID d'événement individuels, procédez de la façon suivante :

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils** > **Options**.
2. Dans la fenêtre **Options**, accédez à l'onglet **Base de données**.
3. Dans la zone **Modèles de messages de rapport**, cliquez sur **Créer une table**.

La table contenant les modèles des ID d'événement est créée dans la langue système en cours et peut être personnalisée.

Avis : la table doit être effacée avant la génération des modèles. Si les modèles ont été générés tel que décrit pour une langue et qu'un utilisateur génère les modèles d'une autre langue, les modèles de la première langue sont supprimés.

27 SafeGuard Enterprise et BitLocker Drive Encryption

BitLocker Drive Encryption est une fonction de chiffrement de disque complet avec authentification de préinitialisation incluse dans les systèmes d'exploitation Microsoft Windows Vista et Windows 7. Elle est conçue pour protéger les données en permettant un chiffrement du volume d'initialisation.

27.1 Comment SafeGuard Enterprise intègre-t-il BitLocker ?

SafeGuard Enterprise permet à BitLocker Drive Encryption inclus dans une installation Windows Vista ou Windows 7 Entreprise ou Édition intégrale d'être géré via SafeGuard Management Center, comme tout autre client SafeGuard Enterprise natif.

Au cours de l'installation du client SafeGuard Enterprise, la prise en charge BitLocker de la fonction doit être explicitement sélectionnée pour permettre l'intégration à BitLocker.

La gestion centralisée et totalement transparente de BitLocker via SafeGuard Enterprise permet ainsi de l'utiliser dans des environnements informatiques hétérogènes. Non seulement SafeGuard Enterprise intègre parfaitement BitLocker Drive Encryption, mais il l'optimise également de manière significative. Les stratégies de sécurité de BitLocker peuvent être appliquées de manière centralisée via SafeGuard Enterprise. Même des processus critiques, comme la gestion et la récupération de clés, sont disponibles lorsque BitLocker est géré par l'intermédiaire de SafeGuard Enterprise.

Pour plus d'informations sur la prise en charge de l'amélioration BitLocker To Go sous Windows 7 par SafeGuard Enterprise, voir *SafeGuard Enterprise et BitLocker To Go* en page 296.

27.2 Amélioration des fonctionnalités de BitLocker avec SafeGuard Enterprise

Les clients profitent des avantages suivants lorsque BitLocker est géré par l'intermédiaire de SafeGuard Enterprise :

- Des volumes supplémentaires du disque local, en plus de la partition d'initialisation, peuvent être chiffrés par BitLocker.
- Le chiffrement basé sur fichier de SafeGuard Enterprise peut également être appliqué à tous les volumes, supports amovibles inclus.
- Les ordinateurs BitLocker peuvent être gérés en toute simplicité dans SafeGuard Management Center : Les stratégies de sécurité peuvent être mises à jour, distribuées et appliquées automatiquement.
- L'état du chiffrement BitLocker est affiché.
- Le mode d'authentification BitLocker peut être défini.

- Les fonctions d'activation et de sauvegarde de clé BitLocker sont plus simples que dans les environnements Vista natifs.
- Un mécanisme de récupération BitLocker de mots de passe et de fichiers de clés est activé pour les volumes d'initialisation et de non-initialisation.

27.3 Quand utiliser SafeGuard Enterprise sans BitLocker Drive Encryption

La méthode de chiffrement basé sur volume de SafeGuard Enterprise offre des avantages supplémentaires par rapport à BitLocker Drive Encryption comme, par exemple :

- Prend également en charge Windows XP et Vista Business
  (BitLocker prend en charge Vista Enterprise et Ultimate uniquement).
- Pas de partition de disque dur spécifique nécessaire pour l'installation
  (BitLocker requiert une partition propre).
- Prend en charge différentes cartes à puce et clés cryptographiques pour l'authentification de préinitialisation
  (BitLocker ne prend en charge aucune carte à puce, uniquement des cartes mémoire contenant un fichier de clés pouvant être copié).
- Prend en charge et distingue différents utilisateurs pendant l'authentification de préinitialisation
  (BitLocker ne distingue pas les différents utilisateurs).
- Permet de réinitialiser les mots de passe oubliés via le mécanisme de challenge/réponse dynamique et sécurisé
  (BitLocker utilise une clé de récupération à 48 chiffres fixe).
- Est doté d'une interface utilisateur graphique pour l'authentification de préinitialisation
  (BitLocker ne comprend que du texte).
- Accepte des mots de passe et règles de mot de passe complexes et synchronisées avec Windows
  (BitLocker autorise l'utilisation d'un code PIN TPM uniquement).
- Permet un chiffrement basé sur secteur pour les supports amovibles
  (Vista BitLocker ne permet pas de chiffrer un quelconque support amovible. Lorsqu'un client BitLocker est utilisé avec SafeGuard Enterprise, le chiffrement de support amovible basé sur fichier est possible).

27.4 Gestion de clients BitLocker avec SafeGuard Enterprise

Dans SafeGuard Enterprise Management Center, les ordinateurs finaux de BitLocker peuvent être gérés exactement comme n'importe quel ordinateur final natif de SafeGuard. En tant que responsable de la sécurité, vous pouvez définir des stratégies de chiffrement et d'authentification pour les ordinateurs finaux BitLocker et les distribuer.

Lorsque l'ordinateur final BitLocker est enregistré dans SafeGuard Enterprise, des informations concernant l'utilisateur, l'ordinateur, le mode de connexion et l'état du chiffrement sont affichées. Les événements sont également consignés pour les clients BitLocker.

La gestion des clients BitLocker dans SafeGuard Enterprise est transparente, ce qui signifie que les fonctions de gestion fonctionnent en général de façon identique pour les clients BitLocker et SafeGuard Enterprise natifs. Vous pouvez connaître le type d'un ordinateur dans l'**Inventaire** d'un conteneur dans **Utilisateurs et ordinateurs.** La colonne **Type POA** vous indique si l'ordinateur correspondant est un client BitLocker ou un client natif de SafeGuard Enterprise.

27.5 Chiffrement avec BitLocker via SafeGuard Enterprise

Avec la prise en charge de BitLocker Drive Encryption dans SafeGuard Enterprise, vous pouvez chiffrer les éléments suivants :

- volume d'initialisation avec le chiffrement BitLocker et des clés BitLocker ;
- autres volumes avec le chiffrement BitLocker et des clés BitLocker ;
- toute donnée, de support amovible par exemple, avec le chiffrement basé sur fichier de SafeGuard Enterprise et des clés SafeGuard Enterprise.

Notez qu'avec la prise en charge SafeGuard Enterprise BitLocker, les disques durs externes sont gérés comme les autres volumes et non comme des supports amovibles. Ils peuvent ainsi être chiffrés sur volume.

27.5.1 Clés de chiffrement pour BitLocker

Lors d'un chiffrement du volume d'initialisation ou d'autres volumes avec BitLocker via SafeGuard Enterprise, les clés de chiffrement sont toujours générées par BitLocker. Une clé est générée par BitLocker pour chaque volume et ne peut pas être réutilisée. Elle doit être stockée en lieu sûr.

L'avantage lié à l'utilisation de BitLocker avec SafeGuard Enterprise réside dans le fait que, pour chaque clé générée par BitLocker, une clé de sauvegarde est stockée dans la base de données de SafeGuard Enterprise. Ceci permet de définir un mécanisme d'assistance et de récupération similaire au mécanisme de challenge/réponse de SafeGuard Enterprise non disponible.

Il n'est cependant pas possible de sélectionner globalement des clés et de les réutiliser avec des clients SafeGuard Enterprise natifs. Les clés n'apparaissent pas dans SafeGuard Management Center.

Si un volume est déjà chiffré avec BitLocker avant d'installer la prise en charge de BitLocker pour SafeGuard Enterprise, l'administrateur doit sauvegarder les clés du volume précédemment chiffré à l'aide des mécanismes de sauvegarde proposés par Microsoft.

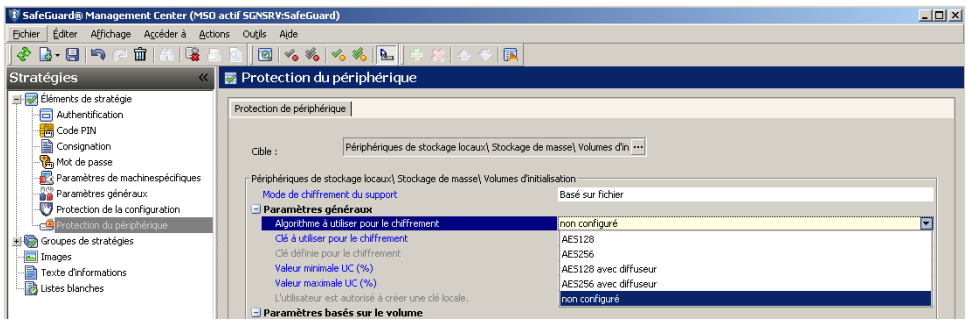
Si un volume est chiffré alors que la prise en charge SafeGuard Enterprise BitLocker est déjà installée, l'administrateur peut enregistrer les clés de sauvegarde (protégées par un mot de passe de récupération) dans Active Directory, en plus du stockage dans la base de données SafeGuard. L'administrateur doit le faire manuellement via l'outil Windows Manage BDE et en les enregistrant dans une stratégie de groupe. Pour Windows 2003 Server, ceci requiert cependant l'extension du schéma Active Directory utilisé, d'où la nécessité de disposer des droits d'administrateur de domaine pour récupérer les informations stockées.

27.5.2 Algorithmes BitLocker dans SafeGuard Enterprise

BitLocker prend en charge les algorithmes AES (Advanced Encryption Standard) suivants :

- AES-128
- AES-256
- AES -128 avec diffuseur
- AES -256 avec diffuseur

Le diffuseur est spécifique à BitLocker et ne peut pas être utilisé en mode de chiffrement basé sur volume de SafeGuard Enterprise. Si un algorithme avec diffuseur est sélectionné pour le chiffrement, tous les modules non-BitLocker de SafeGuard Enterprise utiliseront automatiquement l'algorithme sans diffuseur. Lorsqu'une stratégie est attribuée aux ordinateurs BitLocker et aux ordinateurs SafeGuard Enterprise natifs, ces derniers utiliseront l'algorithme sans diffuseur et les ordinateurs BitLocker utiliseront l'algorithme avec diffuseur.



27.5.3 Stratégies de chiffrement de BitLocker Drive Encryption

Le responsable de la sécurité peut créer une stratégie de chiffrement (initial) dans SafeGuard Management Center et la distribuer aux ordinateurs finaux BitLocker lors de l'exécution.

Les clients BitLocker étant gérés de manière transparente dans Management Center, le responsable de la sécurité ne doit procéder à aucun paramétrage BitLocker spécifique pour le chiffrement. SafeGuard Enterprise détecte l'état des clients et sélectionne le chiffrement BitLocker approprié. Lorsqu'un client BitLocker est installé avec SafeGuard Enterprise et que le chiffrement de volumes est activé, les volumes sont chiffrés par BitLocker Drive Encryption.

27.6 Authentification avec BitLocker Drive Encryption

BitLocker Drive Encryption propose toute une gamme d'options d'authentification. Les utilisateurs BitLocker peuvent s'authentifier via un TPM (Trusted Platform Module) ou une carte mémoire USB ou une combinaison des deux.

Le responsable de la sécurité peut définir les différents modes de connexion dans une stratégie dans SafeGuard Management Center et la distribuer aux ordinateurs de l'utilisateur BitLocker.

Les modes de connexion suivants sont proposés aux utilisateurs SafeGuard Enterprise BitLocker :

- TPM uniquement
- TPM + PIN
- TPM + carte mémoire USB
- Carte mémoire USB uniquement (sans TPM)

TPM (Trusted Platform module)

TPM est un module semblable à une carte à puce sur la carte mère qui exécute des fonctions cryptographiques et des opérations de signature numérique. Il permet de créer, stocker et gérer des clés utilisateur. Il est protégé contre les attaques.

Carte mémoire USB

Les clés externes peuvent être stockées sur une carte mémoire USB non protégée.

27.7 Consignation

Les événements signalés par le client BitLocker sont consignés comme pour tout autre client SafeGuard Enterprise. Il n'est pas expressément indiqué que l'événement est lié à un client BitLocker. Les événements signalés sont identiques pour tout client SafeGuard Enterprise.

28 SafeGuard Enterprise et BitLocker To Go

Avec BitLocker To Go, la fonctionnalité BitLocker Drive Encryption a été étendue dans Microsoft Windows 7 pour permettre aux utilisateurs de chiffrer des volumes internes ainsi que des volumes de supports amovibles pour ordinateurs finaux, via le menu contextuel de l'Explorateur Windows.

- Lorsque le client SafeGuard Enterprise Device Encryption est déployé avec la « prise en charge BitLocker » activée, BitLocker To Go est pris en charge.
- Lorsque le client SafeGuard Enterprise Device Encryption est déployé sans l'activation de la « prise en charge BitLocker » ou lorsque le client SafeGuard Data Exchange est déployé, le chiffrement par BitLocker To Go n'est pas compatible et doit être désactivé dans ce cas. Toutefois, le chiffrement de volumes internes et de supports amovibles peut être configuré de manière centralisée et pratique avec les stratégies de sécurité SafeGuard Enterprise. Les volumes et supports amovibles déjà chiffrés par BitLocker To Go avant le déploiement de SafeGuard Enterprise restent accessibles en lecture.

Pour désactiver le chiffrement BitLocker To Go, procédez comme suit :

1. Dans l'éditeur de stratégies de groupe de Windows, sélectionnez **Stratégie de domaine par défaut** > **Configuration ordinateur** > **Stratégies** > **Modèles d'administration** (**ordinateur local**)> **Composants Windows** > **BitLocker Drive Encryption** > **Supports amovibles**.
2. Sous **Supports amovibles**, sélectionnez la stratégie suivante : **Gérer l'utilisation de BitLocker sur les supports amovibles. Définissez les options comme suit :**
   - Sélectionnez **Activé**.
   - Sous **Options**, désélectionnez : **Les utilisateurs peuvent appliquer la protection BitLocker aux supports amovibles**.
   - Sous **Options**, sélectionnez : **Les utilisateurs peuvent arrêter et déchiffrer la protection BitLocker sur les supports amovibles**.
3. Confirmez en cliquant sur **OK**.

Le chiffrement BitLocker To Go est désactivé sur les ordinateurs finaux. Les utilisateurs ne peuvent plus chiffrer de nouveaux volumes via BitLocker To Go. Les volumes chiffrés par BitLocker To Go avant le déploiement du client natif SafeGuard Enterprise Device Encryption restent accessibles en lecture.

Les paramètres de Registre obtenus côté client se présentent comme suit :

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE]

"RDVConfigureBDE"=dword:00000001

"RDVAllowBDE"=dword:00000000

"RDVDisableBDE"=dword:00000001

Ces clés de Registre sont également définies pendant l'installation du client SafeGuard Enterprise Device Encryption de sorte que Bitlocker To Go est également désactivé sur les ordinateurs sans gestion de domaine comme les ordinateurs de groupe de travail ou autonomes.

29 Événements disponibles pour les rapports

Le tableau suivant présente tous les événements pouvant être sélectionnés pour la consignation.

Catégorie	ID d'événement	Description
Système	1005	Service démarré.
Système	1006	Échec du démarrage du service.
Système	1007	Arrêt du service.
Système	1016	Échec du test d'intégrité des fichiers de données.
Système	1017	Destination de consignation non disponible.
Système	1018	Tentative non autorisée de désinstallation de SafeGuard Enterprise.
Authentification	2001	GINA externe identifié et intégré.
Authentification	2002	GINA externe identifié ; échec de l'intégration.
Authentification	2003	Authentification au démarrage active.
Authentification	2004	Authentification au démarrage désactivée.
Authentification	2005	Éveil par appel réseau activé.
Authentification	2006	Éveil par appel réseau désactivé.
Authentification	2007	Challenge créé.
Authentification	2008	Réponse créée.
Authentification	2009	Connexion établie.
Authentification	2010	Échec de la connexion.
Authentification	2011	Utilisateur importé lors de la connexion et marqué comme propriétaire.
Authentification	2012	Utilisateur importé par un propriétaire et marqué comme non-propriétaire.
Authentification	2013	Utilisateur importé par un non-propriétaire et marqué comme non-propriétaire.
Authentification	2014	Utilisateur supprimé en tant que propriétaire.
Authentification	2015	Échec de l'importation de l'utilisateur lors de la connexion.
Authentification	2016	L'utilisateur s'est déconnecté.
Authentification	2017	L'utilisateur a été contraint de se déconnecter.
Authentification	2018	Action effectuée sur le périphérique.

Catégorie	ID d'événement	Description
Authentification	2019	L'utilisateur a initié une modification de mot de passe/code PIN.
Authentification	2020	Modification mot de passe/code PIN de l'utilisateur après la connexion.
Authentification	2021	Qualité du mot de passe/code PIN.
Authentification	2022	La modification du mot de passe/code PIN n'a pas pu être effectuée.
Authentification	2023	LocalCache était corrompu et a été restauré.
Authentification	2024	Configuration non valide de la liste noire des mots de passe.
Authentification	2025	Le code de réponse permettant à l'utilisateur d'afficher le mot de passe a été reçu.
Authentification	2030	L'utilisateur connecté est un compte de service
Authentification	2035	Liste de comptes de service importée.
Authentification	2036	Liste de comptes de service supprimée.
Authentification	2071	L'initialisation du noyau a été menée à bien.
Authentification	2071	Échec de l'initialisation du noyau.
Authentification	2073	Les clés machine ont été envoyées au serveur.
Authentification	2074	Les clés machine n'ont pas pu être envoyées au serveur.
Authentification	2079	L'importation de l'utilisateur dans le noyau a été menée à bien.
Authentification	2080	La suppression de l'utilisateur du noyau a été menée à bien.
Authentification	2081	Échec de l'importation de l'utilisateur dans le noyau.
Authentification	2082	Échec de la suppression de l'utilisateur du noyau.
Authentification	2083	Réponse avec « afficher le mot de passe utilisateur » créée.
Authentification	2084	Réponse pour les clients virtuels créée.
Authentification	2085	Réponse pour les clients autonomes créée.
Authentification	2095	Impossible d'activer l'éveil par appel réseau.
Authentification	2096	Impossible de désactiver l'éveil par appel réseau.
Administration	2500	Lancement de SafeGuard Enterprise Administration.

Catégorie	ID d'événement	Description
Administration	2501	Échec de la connexion à SafeGuard Enterprise Administration.
Administration	2502	Autorisation pour SafeGuard Enterprise Administration refusée.
Administration	2504	Autorisation supplémentaire accordée pour l'action.
Administration	2505	Autorisation supplémentaire refusée.
Administration	2506	Importation de données depuis le répertoire menée à bien.
Administration	2507	Importation de données depuis le répertoire annulée.
Administration	2508	Impossible d'importer des données depuis le répertoire.
Administration	2511	Utilisateur créé.
Administration	2513	Utilisateur modifié.
Administration	2515	Utilisateur supprimé.
Administration	2518	Échec de l'application de l'utilisateur.
Administration	2522	Impossible de supprimer l'utilisateur.
Administration	2525	Machine appliquée.
Administration	2529	Machine supprimée.
Administration	2532	Échec de l'application de la machine.
Administration	2536	Impossible de supprimer la machine.
Administration	2539	OU appliqué.
Administration	2543	OU supprimé.
Administration	2546	Échec de l'application du OU.
Administration	2547	Échec de l'importation du OU.
Administration	2550	Impossible de supprimer le OU.
Administration	2553	Groupe appliqué.
Administration	2555	Groupe modifié.
Administration	2556	Groupe renommé.
Administration	2557	Groupe supprimé.
Administration	2560	Échec de l'application du groupe.
Administration	2562	Impossible de modifier le groupe.
Administration	2563	Impossible de renommer le groupe.

Catégorie	ID d'événement	Description
Administration	2564	Impossible de supprimer le groupe.
Administration	2573	Membres ajoutés au groupe.
Administration	2575	Membres supprimés du groupe.
Administration	2576	Impossible d'ajouter les membres au groupe.
Administration	2578	Impossible de supprimer les membres du groupe.
Administration	2580	Groupe déplacé d'un OU vers un autre.
Administration	2583	Impossible de passer le groupe d'un OU vers un autre.
Administration	2591	Objets ajoutés au groupe.
Administration	2593	Objets supprimés du groupe.
Administration	2594	Impossible d'ajouter les objets au groupe.
Administration	2596	Impossible de supprimer les objets du groupe.
Administration	2603	Clé générée. Algorithme.
Administration	2607	Clé attribuée.
Administration	2608	Attribution de clé annulée.
Administration	2609	Impossible de générer la clé.
Administration	2613	Impossible d'attribuer la clé.
Administration	2614	Impossible de supprimer l'attribution de la clé.
Administration	2615	Certificat généré.
Administration	2616	Certificat importé.
Administration	2619	Certificat supprimé.
Administration	2621	Certificat attribué à l'utilisateur.
Administration	2622	Annulation de l'attribution de certificat à l'utilisateur.
Administration	2623	Impossible de créer le certificat.
Administration	2624	Impossible d'importer le certificat.
Administration	2627	Impossible de supprimer le certificat.
Administration	2628	Échec de l'extension du certificat.
Administration	2629	Impossible d'attribuer le certificat à l'utilisateur.
Administration	2630	Impossible de supprimer l'attribution du certificat à l'utilisateur.
Administration	2631	Clé cryptographique connectée.

Catégorie	ID d'événement	Description
Administration	2632	Clé cryptographique supprimée.
Administration	2633	Clé cryptographique générée pour l'utilisateur.
Administration	2634	Changer le code PIN utilisateur sur la clé cryptographique.
Administration	2635	Changer le code PIN SO sur la clé cryptographique.
Administration	2636	Clé cryptographique verrouillée.
Administration	2637	Clé cryptographique déverrouillée.
Administration	2638	Clé cryptographique supprimée.
Administration	2639	Attribution de clé cryptographique supprimée pour l'utilisateur.
Administration	2640	Impossible de générer une clé cryptographique pour l'utilisateur.
Administration	2641	Impossible de modifier le code PIN utilisateur sur la clé cryptographique.
Administration	2642	Impossible de modifier le code PIN SO sur la clé cryptographique.
Administration	2643	Impossible de verrouiller la clé cryptographique.
Administration	2644	Impossible de déverrouiller la clé cryptographique.
Administration	2645	Impossible de supprimer la clé cryptographique.
Administration	2647	Stratégie créée.
Administration	2648	Stratégie modifiée.
Administration	2650	Stratégie supprimée.
Administration	2651	Stratégie attribuée et activée sur le OU.
Administration	2652	Stratégie attribuée supprimée du OU.
Administration	2653	Impossible de créer la stratégie.
Administration	2654	Impossible de modifier la stratégie.
Administration	2657	Échec de l'attribution et de l'activation d'une stratégie sur le OU.
Administration	2658	Échec de la suppression de la stratégie attribuée du OU.
Administration	2659	Groupe de stratégies créé.
Administration	2660	Groupe de stratégies modifié.
Administration	2661	Groupe de stratégies supprimé.

Catégorie	ID d'événement	Description
Administration	2662	Impossible de créer le groupe de stratégies.
Administration	2663	Impossible de modifier le groupe de stratégies.
Administration	2665	La stratégie suivante a été ajoutée au groupe de stratégies.
Administration	2667	La stratégie suivante a été supprimée du groupe de stratégies.
Administration	2668	Impossible d'ajouter la stratégie au groupe de stratégies.
Administration	2670	Impossible de supprimer la stratégie du groupe de stratégies.
Administration	2678	Événement enregistré exporté.
Administration	2679	Échec d'exportation des événements enregistrés.
Administration	2680	Événements enregistrés supprimés.
Administration	2681	Impossible de supprimer les événements enregistrés.
Administration	2684	Le responsable de la sécurité autorise le renouvellement du certificat.
Administration	2685	Le responsable de la sécurité refuse le renouvellement du certificat.
Administration	2686	Impossible de modifier les paramètres de renouvellement du certificat.
Administration	2687	Modification du certificat du responsable.
Administration	2688	Impossible de modifier le certificat du responsable.
Administration	2692	Création de groupes de travail.
Administration	2693	Création de groupes de travail impossible.
Administration	2694	Suppression de groupes de travail.
Administration	2695	Suppression de groupes de travail impossible.
Administration	2696	Création d'utilisateurs.
Administration	2697	Création d'utilisateurs impossible.
Administration	2698	Création de machines.
Administration	2699	Création de machines impossible.
Administration	2700	Violation de la licence.
Administration	2701	Création du fichier de clés.
Administration	2702	Suppression de la clé du fichier de clés.

Catégorie	ID d'événement	Description
Administration	2703	Le responsable de la sécurité a désactivé l'authentification au démarrage dans la stratégie.
Administration	2704	Sujet de la question LSH créé.
Administration	2705	Sujet de la question LSH modifié.
Administration	2706	Sujet de la question LSH supprimé.
Administration	2707	Question modifiée.
Administration	2810	Compte d'accès à l'authentification au démarrage « %1 » créé.
Administration	2811	Compte d'accès à l'authentification au démarrage « %1 » modifié.
Administration	2812	Compte d'accès à l'authentification au démarrage « %1 » supprimé.
Administration	2815	Échec de la création du compte d'accès à l'authentification au démarrage « %1 ».
Administration	2816	Échec de la modification du compte d'accès à l'authentification au démarrage « %1 ».
Administration	2817	Échec de la suppression du compte d'accès à l'authentification au démarrage « %1 ».
Administration	2820	Groupe de comptes d'accès à l'authentification au démarrage « %1 » créé.
Administration	2821	Groupe de comptes d'accès à l'authentification au démarrage « %1 » modifié.
Administration	2822	Groupe de comptes d'accès à l'authentification au démarrage « %1 » supprimé.
Administration	2825	Échec de la création du groupe de comptes d'accès à l'authentification au démarrage « %1 ».
Administration	2826	Échec de la modification du groupe de comptes d'accès à l'authentification au démarrage « %1 ».
Administration	2827	Échec de la suppression du groupe de comptes d'accès à l'authentification au démarrage « %1 ».
Client	3003	Sauvegarde du noyau réussie.
Client	3005	Première tentative de restauration du noyau réussie.
Client	3006	Deuxième tentative de restauration du noyau réussie.
Client	3007	Échec de la sauvegarde du noyau.

Catégorie	ID d'événement	Description
Client	3008	Échec de la restauration du noyau.
Client	3030	L'utilisateur a modifié ses secrets LSH après la connexion.
Client	3035	Activation de LSH.
Client	3040	Désactivation de LSH.
Client	3045	LSH est disponible : client Enterprise
Client	3046	LSH est disponible : client autonome
Client	3050	Désactivation de LSH : client Enterprise
Client	3051	LSH n'est pas disponible : client autonome
Client	3055	La liste QST (questions LSH) a été modifiée.
Client	3405	La désinstallation du client de protection de configuration a échoué.
Client	3070	La sauvegarde de clé a été enregistrée dans le partage réseau spécifié.
Client	3071	La sauvegarde de clé n'a pas pu être enregistrée dans le partage réseau spécifié.
Client	3110	Compte d'accès à l'authentification au démarrage « %1 » importé dans POA.
Client	3111	Compte d'accès à l'authentification au démarrage « %1 » supprimé de POA.
Client	3115	Compte d'accès à l'authentification au démarrage « %1 » : modification du mot de passe via la touche F8.
Client	3116	Échec de l'importation du compte d'accès à l'authentification au démarrage « %1 » dans POA.
Client	3117	Échec de la suppression du compte d'accès à l'authentification au démarrage « %1 » de POA.
Client	3118	Compte d'accès à l'authentification au démarrage « %1 » : échec de la modification du mot de passe via la touche F8.
Client	3406	Une erreur s'est produite au niveau du client de protection de configuration.
Client	3407	Le client de protection de configuration a détecté une possible falsification.
Client	3408	Le client de protection de configuration a détecté une possible falsification des fichiers journaux.

Catégorie	ID d'événement	Description
Chiffrement	3501	Accès refusé au support sur le lecteur.
Chiffrement	3502	Accès refusé au fichier de données.
Chiffrement	3503	Démarrage du chiffrement initial basé sur secteur du lecteur.
Chiffrement	3504	Démarrage du chiffrement initial basé sur secteur du lecteur (mode rapide).
Chiffrement	3505	Fin du chiffrement initial basé sur secteur du lecteur réussie.
Chiffrement	3506	Échec et clôture du chiffrement initial basé sur secteur du lecteur.
Chiffrement	3507	Annulation du chiffrement initial basé sur secteur du lecteur.
Chiffrement	3508	Échec du chiffrement initial basé sur secteur du lecteur.
Chiffrement	3509	Démarrage du déchiffrement basé sur secteur du lecteur.
Chiffrement	3510	Clôture du déchiffrement basé sur secteur du lecteur réussie.
Chiffrement	3511	Échec et clôture du déchiffrement basé sur secteur du lecteur.
Chiffrement	3512	Annulation du déchiffrement basé sur secteur du lecteur.
Chiffrement	3513	Échec du déchiffrement basé sur secteur du lecteur.
Chiffrement	3514	Démarrage du chiffrement initial F&F sur le lecteur.
Chiffrement	3515	Fin du chiffrement initial F&F sur le lecteur réussie.
Chiffrement	3516	Échec et clôture du chiffrement initial F&F sur le lecteur.
Chiffrement	3517	Annulation du déchiffrement F&F sur le lecteur.
Chiffrement	3519	Démarrage du chiffrement F&F.
Chiffrement	3520	Clôture du chiffrement F&F réussie.
Chiffrement	3521	Échec et clôture du déchiffrement F&F.
Chiffrement	3522	Annulation du déchiffrement F&F sur le lecteur.
Chiffrement	3524	Démarrage du chiffrement F&F.
Chiffrement	3525	Fin du chiffrement F&F réussie.

Catégorie	ID d'événement	Description
Chiffrement	3526	Échec du chiffrement F&F.
Chiffrement	3540	Démarrage du déchiffrement F&F.
Chiffrement	3541	Fin du déchiffrement F&F réussie.
Chiffrement	3542	Échec du déchiffrement F&F.
Chiffrement	3543	Sauvegarde de la clé d'initialisation réussie.
Chiffrement	3544	Nombre maximum d'algorithmes d'initialisation dépassé.
Chiffrement	3545	Erreurs de lecture sur la KSA.
Chiffrement	3546	Désactivation des volumes en fonction des stratégies définies.
Chiffrement	3560	Contrôle d'accès
Chiffrement	3600	Erreur générale de chiffrement
Chiffrement	3601	Erreur de chiffrement - moteur : volume manquant.
Chiffrement	3602	Erreur de chiffrement - moteur : volume hors ligne.
Chiffrement	3603	Erreur de chiffrement - moteur : volume supprimé.
Chiffrement	3604	Erreur de chiffrement - moteur : volume incorrect.
Chiffrement	3607	Erreur de chiffrement - clé de chiffrement manquante.
Chiffrement	3610	Erreur de chiffrement - zone de stockage des clés d'origine endommagée
Chiffrement	3611	Erreur de chiffrement - zone de stockage des clés de sauvegarde endommagée sur le volume
Chiffrement	3612	Erreur de chiffrement - zone ESA d'origine endommagée sur le volume
Contrôle d'accès	4400	Le port a été approuvé.
Contrôle d'accès	4401	Le périphérique a été approuvé.
Contrôle d'accès	4402	Le périphérique de stockage a été approuvé.
Contrôle d'accès	4403	Le réseau local sans fil a été approuvé.
Contrôle d'accès	4404	Le port a été retiré avec succès.
Contrôle d'accès	4405	Le périphérique a été retiré avec succès.
Contrôle d'accès	4406	Le périphérique de stockage a été retiré avec succès.
Contrôle d'accès	4407	Le réseau local sans fil a été déconnecté avec succès.
Contrôle d'accès	4408	Port restreint

Catégorie	ID d'événement	Description
Contrôle d'accès	4409	Périphérique restreint
Contrôle d'accès	4410	Périphérique de stockage restreint
Contrôle d'accès	4411	Réseau local sans fil restreint
Contrôle d'accès	4412	Port bloqué
Contrôle d'accès	4413	Périphérique bloqué
Contrôle d'accès	4414	Périphérique de stockage bloqué
Contrôle d'accès	4415	Réseau local sans fil bloqué

30 Définition des codes SGMERR du journal des événements de Windows

Le message suivant s'affichera dans le journal des événements de Windows :

« Autorisation pour SafeGuard Enterprise Administration refusée pour l'utilisateur... Motif : SGMERR[536870951] »

Consultez le tableau ci-dessous pour connaître la définition du numéro « 536870951 ». Le numéro « 536870951 » signifie par exemple « Saisie incorrecte du code PIN. Authentification impossible de l'utilisateur ».

ID de l'erreur :	Affichage
0	OK
1	Erreur du paramètre 1
2	Erreur du paramètre 2
3	Erreur du paramètre 3
4	Erreur du paramètre 4
5	Erreur du paramètre 5
6	Erreur du paramètre 6
7	Erreur du paramètre 7
8	Erreur du paramètre 8
9	Erreur du paramètre 9
10	Erreur du paramètre 10
11	Erreur du paramètre 11
12	Erreur du paramètre 12
13	Erreur du paramètre 13
14	Erreur du paramètre 14
15	Erreur du paramètre 15
16	Erreur du paramètre 16
17	Erreur du paramètre 17
18	Erreur du paramètre 18
19	Erreur du paramètre 19
20	La fonction n'a pas été exécutée
21	Erreur interne détectée

22	Module non initialisé
23	Erreur d'E/S de fichier détectée
24	Le cache ne peut pas être attribué
25	Erreur de lecture d'E/S de fichier
26	Erreur d'écriture d'E/S de fichier
50	Aucune opération n'a été effectuée
101	Erreur générale
102	Accès refusé
103	Le fichier existe déjà
1201	Impossible d'ouvrir l'entrée du registre.
1202	Impossible de lire l'entrée du registre.
1203	Impossible d'écrire l'entrée du registre.
1204	Impossible de supprimer l'entrée du registre.
1205	Impossible de créer l'entrée du registre.
1206	Accès impossible à un pilote ou un service système.
1207	Impossible d'ajouter un pilote ou un service système dans le registre.
1208	Impossible de supprimer un pilote ou un service système du registre.
1209	Une entrée est déjà présente dans le registre pour un pilote ou un service système.
1210	Aucun accès au Service Control Manager.
1211	Impossible de trouver une entrée dans le registre pour une session.
1212	Une entrée du registre est non valide ou erronée.
1301	Échec de l'accès à un lecteur.
1302	Aucune information n'est disponible sur un volume.
1303	Échec de l'accès à un volume.
1304	Option non valide définie.
1305	Type de système de fichiers non valide.
1306	Le système de fichiers existant sur un volume et le système de fichiers défini diffèrent.
1307	La taille de cluster existante utilisée par un système de fichiers et la taille de cluster définie diffèrent.
1308	Taille de secteur non valide utilisée par un système de fichier défini.

1309	Secteur de départ non valide défini.
1310	Type de partition non valide défini.
1311	Impossible de trouver une zone non utilisée et défragmentée de la taille requise sur un volume.
1312	Impossible de marquer le cluster du système de fichiers comme étant utilisé.
1313	Impossible de marquer le cluster du système de fichiers comme étant utilisé.
1314	Impossible de marquer le cluster du système de fichiers comme étant CORRECT.
1315	Impossible de marquer le cluster du système de fichiers comme étant INCORRECT.
1316	Aucune information disponible sur les clusters d'un système de fichiers.
1317	Impossible de trouver une zone marquée comme MAUVAISE sur un volume.
1318	Taille non valide d'une zone sur un volume défini.
1319	Le secteur MBR d'un disque dur n'a pas pu être remplacé.
1330	Une commande erronée a été définie pour une allocation ou une désallocation.
1351	Algorithme non valide défini.
1352	Échec de l'accès au noyau système.
1353	Aucun noyau système n'est installé.
1354	Une erreur s'est produite lors de l'accès au noyau système.
1355	Modification non valide des paramètres système.
1401	Échec de l'écriture de données sur un lecteur.
1402	Échec de la lecture de données d'un lecteur.
1403	Échec de l'accès à un lecteur.
1404	Lecteur non valide défini.
1405	Échec du changement de position sur un lecteur.
1406	Le lecteur n'est pas prêt.
1407	Échec du démontage d'un lecteur.
1451	Impossible d'ouvrir le fichier.
1452	Le fichier est introuvable.
1453	Le chemin d'accès défini pour le fichier est non valide.

1454	Impossible de créer le fichier.
1455	Impossible de copier le fichier.
1456	Aucune information n'est disponible sur un volume.
1457	Impossible de modifier la position dans un fichier.
1458	Échec de la lecture de données d'un fichier.
1459	Échec de l'écriture de données dans un fichier.
1460	Impossible de supprimer un fichier.
1461	Système de fichiers non valide.
1462	Impossible de fermer le fichier.
1463	L'accès à un fichier a été refusé.
1501	Mémoire disponible insuffisante.
1502	Paramètre non valide ou erroné défini.
1503	Dépassement de la taille de la mémoire tampon de données.
1504	Un module DLL n'a pas pu être chargé.
1505	Une fonction ou un processus a été annulé.
1506	Aucun accès autorisé.
1510	Aucun noyau système n'est installé.
1511	Impossible de lancer un programme.
1512	Une fonction, un objet ou une donnée est indisponible.
1513	Entrée non valide détectée.
1514	Un objet existe déjà.
1515	Appel de fonction non valide.
1516	Une erreur interne s'est produite.
1517	Une violation d'accès s'est produite.
1518	La fonction ou le mode n'est pas pris en charge.
1519	Échec de la désinstallation.
1520	Une erreur d'exception s'est produite.
1550	Le secteur MBR du disque dur n'a pas pu être remplacé.
20001	Inconnu
20002	Processus terminé
20003	Fichier non vérifié

20004	Stratégie non valide
30050	Impossible d'ouvrir la commande
30051	Mémoire insuffisante
30052	Échec général de la communication de traitement
30053	Une ressource est temporairement indisponible. Cet état est temporaire. Des tentatives d'accès ultérieures peuvent fonctionner normalement.
30054	Échec général de communication
30055	Valeur renvoyée inattendue
30056	Aucun lecteur de carte n'est connecté.
30057	Dépassement de mémoire tampon
30058	La carte n'est pas alimentée
30059	Un dépassement de délai s'est produit
30060	Type de carte incorrect
30061	La fonctionnalité demandée n'est pas prise en charge à l'heure actuelle / par ce SE / dans cette situation, etc.
30062	Pilote non valide
30063	Ce logiciel ne peut pas utiliser le microprogramme du matériel connecté
30064	Impossible d'ouvrir le fichier
30065	Fichier introuvable
30066	La carte n'est pas insérée
30067	Argument non valide
30068	Le sémaphore est en cours d'utilisation
30069	Le sémaphore est temporairement en cours d'utilisation
30070	Échec général
30071	Actuellement, vous ne disposez pas des droits permettant d'effectuer l'opération demandée. Généralement, un mot de passe doit être fourni au préalable.
30072	Actuellement, le service n'est pas disponible
30073	Un élément (par ex. une clé portant un nom spécifique) est introuvable
30074	Le mot de passe fourni est incorrect.
30075	Le mot de passe fourni plusieurs fois est incorrect, l'accès est par conséquent verrouillé. Il est généralement possible d'utiliser un outil d'administration approprié pour le déverrouiller.

30076	L'identité ne correspond pas à une identité définie ayant fait l'objet d'un contrôle croisé
30077	Plusieurs erreurs se sont produites. Utilisez ce code d'erreur si c'est le seul moyen d'obtenir un code d'erreur lorsque des erreurs différentes se sont produites.
30078	Il reste des éléments, par conséquent la structure du répertoire ne peut par ex. pas être supprimée.
30079	Erreur lors du contrôle de cohérence
30080	L'ID se trouve sur une liste noire, par conséquent, l'opération demandée n'est pas autorisée.
30081	Identificateur non valide
30082	Fichier de configuration non valide
30083	Secteur introuvable.
30084	Entrée introuvable.
30085	Plus de sections
30086	Fin du fichier atteinte.
30087	L'élément spécifié existe déjà
30088	Le mot de passe fourni est trop court.
30089	Le mot de passe fourni est trop long.
30090	Un élément (par ex. un certificat) a expiré
30091	Le mot de passe n'est pas verrouillé.
30092	Chemin introuvable.
30093	Le répertoire n'est pas vide.
30094	Aucune donnée supplémentaire
30095	Le disque est plein.
30096	Une opération a été annulée.
30097	Données en lecture seule ; échec d'une opération d'écriture.
12451840	La clé n'est pas disponible.
12451842	La clé n'est pas définie.
12451842	Accès refusé au support non chiffré.
12451843	Accès refusé au support non chiffré sauf s'il est vide.
352321637	Le fichier n'est pas chiffré.
352321638	La clé n'est pas disponible.

352321639	La clé correcte n'est pas disponible.
352321640	Erreur de la somme de contrôle dans l'en-tête du fichier.
352321641	Erreur de la fonction CBI.
352321642	Nom de fichier non valide.
352321643	Erreur de lecture/écriture du fichier temporaire.
352321644	L'accès aux données non chiffrées n'est pas autorisé.
352321645	Zone de stockage des clés (KSA) saturée.
352321646	Le fichier est déjà chiffré avec un autre algorithme.
352321647	Le fichier est compressé avec NTFS et ne peut pas être chiffré.
352321648	Le fichier est chiffré avec EFS.
352321649	Propriétaire du fichier non valide
352321650	Mode de chiffrement du fichier non valide
352321651	Erreur d'opération CBC.
385875969	Intégrité rompue.
402653185	La clé cryptographique ne contient pas d'informations d'identification.
402653186	Impossible d'écrire les informations d'identification sur la clé cryptographique.
402653187	Impossible de créer la balise TDF.
402653188	La balise TDF ne contient pas les données requises.
402653189	L'objet existe déjà sur la clé cryptographique.
402653190	Aucun slot valide trouvé
402653191	Lecture impossible du numéro de série
402653192	Le chiffrement de la clé cryptographique a échoué.
402653193	Le déchiffrement de la clé cryptographique a échoué.
536870913	Le fichier de clés ne contient pas de données valides.
536870914	Des parties de la paire de clés RSA sont incorrectes
536870915	Impossible d'importer la paire de clés.
536870916	Le format du fichier de clés n'est pas valide.
536870917	Aucune donnée disponible
536870918	Échec de l'importation du certificat.
536870919	Le module a déjà été initialisé
536870920	Le module n'a pas encore été initialisé

536870921	Le chiffrement ASN.1 est corrompu.
536870922	Longueur des données incorrecte
536870923	Signature incorrecte.
536870924	Mécanisme de chiffrement appliqué incorrect.
536870925	Cette version n'est pas prise en charge.
536870926	Erreur de remplissage.
536870927	Indicateurs non valides.
536870928	Le certificat a expiré et n'est plus valide
536870929	Heure saisie incorrecte. Le certificat n'est pas encore valide.
536870930	Le certificat a été retiré.
536870931	La chaîne de certificat est non valide.
536870932	Impossible de créer la chaîne de certificat.
536870933	Impossible de contacter CDP.
536870934	Un certificat pouvant être utilisé uniquement comme unité de donnée finale a été utilisé comme CA ou réciproquement.
536870935	Problèmes de validité de la longueur du certificat dans la chaîne.
536870936	Erreur d'ouverture d'un fichier.
536870937	Erreur de lecture d'un fichier.
536870938	Un ou plusieurs paramètres attribués à la fonction sont incorrects.
536870939	Le résultat de la fonction dépasse la taille du cache.
536870940	Problème de clé cryptographique et/ou slot rompu.
536870941	La clé cryptographique n'a pas suffisamment de mémoire pour effectuer la fonction demandée.
536870942	La clé cryptographique a été retirée du slot alors que la fonction était en cours.
536870943	La fonction demandée n'a pas pu être réalisée, mais aucune information concernant la cause de cette erreur n'est disponible.
536870945	L'ordinateur sur lequel la compilation CBI s'effectue n'a pas suffisamment de mémoire pour effectuer la fonction demandée. Il se peut que cette fonction ne soit que partiellement exécutée.
536870946	Une opération demandée n'est pas prise en charge par la compilation CBI.
536870947	Tentative de définition d'une valeur pour un objet qui ne peut pas être paramétré ou modifié.
536870948	Valeur non valide pour l'objet.

536870949	Échec d'obtention de la valeur d'un objet car celui-ci est sensible ou inaccessible.
536870950	Le code PIN saisi a expiré. (Le fait que le code PIN d'un utilisateur classique fonctionne ou non sur une clé cryptographique générée dépend de cette dernière).
536870951	Le code PIN fourni est incorrect. Authentification impossible de l'utilisateur.
536870952	Le code PIN saisi contient des caractères non valides. Ce code de réponse ne s'applique qu'aux opérations qui tentent de définir un code PIN.
536870953	Le code PIN saisi est trop long ou trop court. Ce code de réponse ne s'applique qu'aux opérations qui tentent de définir un code PIN.
536870954	Le code PIN sélectionné est bloqué et ne peut pas être utilisé. Ceci se produit lorsqu'un certain nombre de tentatives ont été faites pour authentifier un utilisateur et lorsque la clé cryptographique refuse toute tentative supplémentaire.
536870955	ID de slot non valide.
536870956	La clé cryptographique n'était pas dans le slot lors de la requête.
536870957	L'archive CBI et/ou le slot n'ont pas reconnu la clé cryptographique qui s'y trouve.
536870958	L'opération demandée n'a pas pu être effectuée car la clé cryptographique est protégée en écriture.
536870959	L'utilisateur saisi ne peut pas se connecter car il est déjà connecté à une session.
536870960	L'utilisateur saisi ne peut pas se connecter car un autre utilisateur est déjà connecté à cette session.
536870961	L'opération demandée n'a pas pu être effectuée car aucun utilisateur correspondant n'est connecté. Par exemple, il n'est pas possible de quitter une session lorsqu'un utilisateur est encore connecté.
536870962	Le code PIN de l'utilisateur normal n'a pas été initialisé avec CBIInitPin
536870963	Une tentative de connexion effectuée par plusieurs utilisateurs simultanément sur la même clé cryptographique a été autorisée.
536870964	Une valeur incorrecte a été spécifiée en tant que CBIUser. Les types valides sont définis dans les types d'utilisateurs.
536870965	Un objet ayant l'ID spécifié est introuvable sur la clé cryptographique.
536870966	Dépassement de délai de l'opération.
536870967	Cette version d'IE n'est pas prise en charge
536870968	Échec d'authentification

536870969	Le certificat de base n'est pas sécurisé.
536870970	Aucune CRL trouvée
536870971	Aucune connexion Internet active.
536870972	Erreur de valeur de temps du certificat.
536870973	Impossible de vérifier le certificat sélectionné.
536870974	Le statut d'expiration du certificat est inconnu.
536870975	Le module s'est fermé. Aucune autre demande.
536870976	Une erreur s'est produite pendant la requête d'une fonction réseau.
536870977	Une requête de fonction non valide a été reçue.
536870978	Impossible de trouver un objet.
536870979	Une session terminal server a été interrompue.
536870980	Opération non valide.
536870981	L'objet est en cours d'utilisation
536870982	Le générateur de nombres aléatoire n'a pas été initialisé. (CBIRNDInit ( ) non requis.)
536870983	Commande inconnue (voir CBIControl ( ))
536870984	UNICODE n'est pas pris en charge
536870985	Davantage de valeurs de départ sont nécessaires pour le générateur de nombres aléatoire
536870986	L'objet existe déjà
536870987	Combinaison d'algorithme incorrecte. (Voir CBIRecrypt ( )).
536870988	Le module Cryptoki (PKCS#11) n'a pas été initialisé.
536870989	Le module Cryptoki (PKCS#11) a été initialisé.
536870990	Impossible de charger le module Cryptoki (PKCS#11).
536870991	Certificat introuvable
536870992	Non approuvé
536870993	Clé non valide
536870994	La clé ne peut pas être exportée.
536870995	L'algorithme spécifié n'est pas pris en charge temporairement.
536870996	Le mode de déchiffrement saisi n'est pas pris en charge.
536870997	Erreur de compilation GSENC.
536870998	Le format de requête de données n'est pas reconnu.

536870999	Le certificat n'a pas de clé privée.
536871000	Paramètre système incorrect.
536871001	Une opération est active.
536871002	Un certificat de la chaîne n'est pas correctement imbriqué.
536871003	La CRL n'a pas pu être remplacée.
536871004	Le code PIN de l'utilisateur a déjà été initialisé.
805306369	Vous ne disposez pas des droits permettant d'effectuer cette opération. Accès refusé.
805306370	Opération non valide
805306371	Paramètre utilisé non valide
805306372	L'objet existe déjà
805306373	L'objet est introuvable.
805306374	Exception de la base de données
805306375	L'opération a été annulée par l'utilisateur
805306376	La clé cryptographique n'est pas attribuée à un utilisateur spécifique
805306377	La clé cryptographique est attribuée à plusieurs utilisateurs
805306378	La clé cryptographique est introuvable dans la base de données
805306379	La clé cryptographique a été supprimée et retirée de la base de données
805306380	Impossible d'identifier la clé cryptographique dans la base de données.
805306381	La stratégie est attribuée à un groupe de stratégies. Supprimez l'attribution avant de supprimer la stratégie.
805306382	La stratégie est attribuée à un OU. Supprimez d'abord l'attribution.
805306383	Le certificat n'est pas valide pour ce responsable.
805306384	Le certificat a expiré pour ce responsable.
805306385	Le responsable est introuvable dans la base de données.
805306386	Le responsable sélectionné n'est pas unique.
805306387	Le responsable est bloqué et ne peut pas être authentifié.
805306388	Le responsable n'est plus ou n'est pas encore valide.
805306389	Impossible d'autoriser le responsable - requête en dehors des heures de bureau.
805306390	Une partie responsable ne peut pas se supprimer.

805306391	Le responsable principal de la sécurité ne peut pas être supprimé car un second responsable principal de la sécurité est nécessaire pour une authentification supplémentaire.
805306392	Le responsable de la sécurité ne peut pas être supprimé car un second responsable de la sécurité est requis pour une authentification supplémentaire.
805306393	Le responsable de la vérification ne peut pas être supprimé car un second responsable de la vérification est requis pour une authentification supplémentaire.
805306394	Le responsable récupération ne peut pas être supprimé car un second responsable récupération est requis pour une authentification supplémentaire.
805306395	Le responsable conseil ne peut pas être supprimé car un second responsable conseil est requis pour une authentification supplémentaire.
805306396	La fonction de responsable principal de la sécurité ne peut pas être supprimée car un second responsable principal de la sécurité est nécessaire pour une authentification supplémentaire.
805306397	La fonction de responsable de la sécurité ne peut pas être supprimée car un second responsable de la sécurité est nécessaire pour une authentification supplémentaire.
805306398	La fonction de responsable de la vérification ne peut pas être supprimée car un second responsable de la vérification est nécessaire pour une authentification supplémentaire.
805306399	La fonction de responsable récupération ne peut pas être supprimée car un second responsable récupération est nécessaire pour une authentification supplémentaire.
805306400	La fonction de responsable récupération ne peut pas être supprimée car un second responsable récupération est nécessaire pour une authentification supplémentaire.
805306401	Aucun responsable supplémentaire ayant la fonction requise n'est disponible pour une authentification supplémentaire.
805306402	Journal des événements
805306403	L'intégrité du journal des événements central a été vérifiée.
805306404	Intégrité rompue. Un ou plusieurs événements ont été supprimés du début de la chaîne.
805306405	Intégrité rompue. Un ou plusieurs événements ont été supprimés de la chaîne. Le message indiquant la détection du point de rupture de la chaîne a été mis en surbrillance.

805306406	Intégrité rompue. Un ou plusieurs événements ont été supprimés de la fin de la chaîne.
805306407	Impossible d'exporter les événements dans le fichier. Motif :
805306408	L'affichage actuel comprend des données non enregistrées. Voulez-vous enregistrer les modifications avant de quitter cet affichage ?
805306409	Le fichier n'a pas pu être chargé ou est endommagé. Motif :
805306410	L'intégrité du journal a été rompue. Un ou plusieurs événements ont été supprimés.
805306411	Voulez-vous enregistrer les événements dans un fichier avant de les supprimer ?
805306412	Affichage des tâches
805306413	Plusieurs CRL trouvées dans la base de données : Impossible de supprimer les CRL.
805306414	CRL introuvable dans la base de données :
805306415	L'utilisateur auquel le certificat devrait avoir été attribué est introuvable dans la base de données.
805306416	Un blob P7 est requis en urgence pour l'attribution d'un certificat.
805306417	L'utilisateur auquel le certificat devrait avoir été attribué n'a pas un nom unique.
805306418	Il est malheureusement impossible de trouver l'attribution du certificat.
805306419	L'attribution du certificat n'est pas unique. Le certificat devant être supprimé n'est pas clair.
805306420	L'utilisateur pour lequel le certificat doit être produit est introuvable dans la base de données.
805306421	L'utilisateur auquel le certificat doit être attribué ne peut pas avoir un nom unique.
805306422	Le certificat a déjà été attribué à un autre utilisateur. Un certificat ne peut être attribué qu'à un seul utilisateur.
805306423	La machine à laquelle le certificat doit être attribué est introuvable dans la base de données.
805306424	La machine à laquelle le certificat doit être attribué n'a pas pu être identifiée de façon unique.
805306425	Les certificats importés ne peuvent pas être étendus par SGN.
805306426	Données de certificat incohérentes
805306427	L'extension du certificat n'a pas été approuvée par un responsable de la sécurité.

805306428	Erreur de suppression de la clé cryptographique
805306429	Le certificat ne peut pas être supprimé par la clé cryptographique car il a été autorisé par l'utilisateur présent.
805306430	Un accès système du même nom existe déjà. Sélectionnez un autre nom.
805306431	Aucun rôle n'est affecté au responsable de la sécurité. La connexion est impossible.
805306432	La licence a été violée.
805306433	Aucune licence trouvée.
2415919104	Aucune stratégie trouvée.
2415919105	Aucun fichier de configuration n'est disponible.
2415919106	Aucune connexion au serveur.
2415919107	Aucune donnée supplémentaire.
2415919108	Priorité non valide utilisée pour l'envoi au serveur.
2415919109	Données supplémentaires en attente.
2415919110	Enregistrement automatique en attente.
2415919111	Échec de l'authentification de la base de données.
2415919112	ID de session erroné.
2415919113	Paquet de données ignoré.
3674210305	Domaine introuvable.
3674210306	Machine introuvable.
3674210307	Utilisateur introuvable.
3758096385	Le mot de passe ne contient pas assez de lettres
3758096386	Le mot de passe ne contient pas assez de chiffres
3758096387	Le mot de passe ne contient pas assez de caractères spéciaux
3758096388	Le mot de passe est identique au nom d'utilisateur
3758096389	Le mot de passe contient des caractères consécutifs
3758096390	Le mot de passe ressemble trop au nom d'utilisateur
3758096391	Le mot de passe figure dans la liste des mots de passe interdits
3758096392	Le mot de passe ressemble trop à l'ancien mot de passe
3758096393	Le mot de passe comporte une séquence clavier de plus de deux caractères
3758096394	Le mot de passe comporte une colonne clavier de plus de deux caractères
3758096395	Le mot de passe n'est pas encore valide

3758096396	Un mot de passe a expiré
3758096397	La période de validité minimum du mot de passe n'est pas expirée
3758096398	La période de validité maximum du mot de passe est expirée
3758096399	Les informations concernant un changement de mot de passe imminent doivent être affichées
3758096400	Doit être changé lors de la première connexion
3758096401	Le mot de passe a été trouvé dans l'historique
3758096402	Erreur lors de la vérification par rapport à la liste noire spécifiée.
4026531840	Aucune « plate-forme » trouvée.
4026531841	Aucun document.
4026531842	Erreur d'analyse XML.
4026531843	Erreur Document Object Model (XML).
4026531844	Aucune balise <DATAROOT> trouvée.
4026531845	Balise XML introuvable.
4026531846	Erreur « nostream ».
4026531847	Erreur « printtree ».

31 Support technique

Vous pouvez obtenir du support technique pour les produits Sophos de l'une des manières suivantes :

- Visitez le forum SophosTalk à l'adresse http://community.sophos.com/ et recherchez d'autres utilisateurs qui connaissent le même problème.
- Visitez la base de connaissances du support technique de Sophos à l'adresse http://www.sophos.fr/support/
- Téléchargez la documentation des produits à l'adresse http://www.sophos.fr/support/docs/
- Envoyez un courriel à support@sophos.com, y compris le(s) numéro(s) de version du ou des logiciels Sophos, le(s) système(s) d'exploitation et le(s) niveau(x) de correctif ainsi que le texte de tout message d'erreur.

32 Copyright

Copyright © 1996 - 2010 Sophos Group et Utimaco Safeware AG. Tous droits réservés.

Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos est une marque déposée de Sophos Plc et de Sophos Group. SafeGuard est une marque déposée de Utimaco Safeware AG - a member of the Sophos Group. Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

Tous les produits SafeGuard sont sous le copyright d'Utimaco Safeware AG- a member of the Sophos Group, ou, le cas échéant, des concédants de la licence. Tous les autres produits Sophos sont sous copyright de Sophos Plc, ou, le cas échéant, des concédants de la licence.

Vous trouverez des informations de copyright des fournisseurs tiers dans le fichier Disclaimer and Copyright for 3rd Party Software.rtf de votre répertoire d'installation.